

416
BIBLIOTECA SOCIETĂȚII DE ȘTIINȚE MATEMATICE ȘI FIZICE DIN R. P. R.

G. N. BERMAN

DESPRE NUMERE

ȘI STUDIUL NUMERELOR

E D I T U R A T E H N I C Ă

G. N. BERMAN

Shuov

**DESPRE NUMERE
ȘI
STUDIUL NUMERELOR**

TRADUCERE DIN LIMBA RUSĂ
DUPĂ EDIȚIA A DOUA REVĂZUTĂ

BIBLIOTECA SOCIETĂȚII DE ȘTIINȚE MATEMATICE ȘI FIZICE DIN R.P.R.



EDITURA TEHNICĂ
BUCUREȘTI 1961

În lucrare sînt prezentate într-o formă accesibilă cîteva capitole din teoria numerelor. Astfel sînt expuse unele sisteme de numerație vechi și noi, divizibilitatea numerelor, numerele prime și proprietățile lor, „mica” și „marea” teoremă a lui Fermat.

Pentru înțelegerea conținutului broșurii sînt necesare doar cunoștințe de aritmetică și algebră elementară. Cartea se adresează elevilor din școlile de cultură generală, studenților din primii ani de studii și profesorilor din învățămîntul mediu și elementar.

Г. Н. Берман

ЧИСЛО И НАУКА О НЁМ

Издание второе Исправленное

ГОСУДАРСТВЕННОЕ ИЗДАТЕЛЬСТВО
ТЕХНИКО-ТЕОРЕТИЧЕСКОЙ ЛИТЕРАТУРЫ

Москва 1954

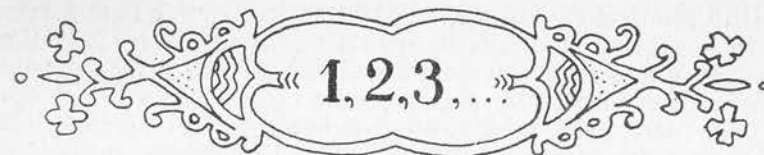
DIN PREFAȚA AUTORULUI LA PRIMA EDIȚIE

Există multe cărți bune, a căror sarcină este de a trezi interesul pentru matematică. Cartea de față are alt scop: ea este destinată acelor care se interesează de matematică, dar nu au suficientă pregătire pentru a citi literatura de specialitate. De aceea, cititorul nu va găsi aici nici șarade matematice, nici anecdote amuzante. Această broșură este consacrată expunerii accesibile, însă serioase, a unor capitole din teoria numerelor întregi. Pentru înțelegerea ei sînt suficiente cunoștințe elementare de aritmetică și de algebră, predate în clasele VIII—IX din școala medie. Autorul s-a străduit să ofere material de lectură profesorilor începători din învățămîntul mediu, studenților de la institutele pedagogice și, mai ales, elevilor care fac parte din cercurile de matematică.

Această carte nu este un manual. De aceea, pentru a face expunerea mai atrăgătoare, autorul a renunțat intenționat la expunerea sistematică a elementelor teoriei numerelor. Poate însă că studenții vor vedea în ea o trambulină comodă pentru a se lansa din confortabila aritmetică elementară în serioasa și pretențioasa teorie a numerelor.

Autorul mulțumește tuturor celor care au contribuit la scrierea și la publicarea acestei cărți. Autorul este deosebit de recunoscător profesorului A. F. Bermant, care a citit cu atenție manuscrisul și i-a dat indicații valoroase.

Moscova, 1947.



INTRODUCERE



oțiunea de număr natural a apărut din necesitatea de a număra, pe primele trepte ale dezvoltării societății umane, cu mult înaintea apariției noțiunilor de număr fracționar și număr negativ. Se numesc naturale numerele unu, doi, trei, patru, cinci, șase etc.

Omul contemporan se familiarizează cu ele începând cu vârsta preșcolară.

Totuși, deși sînt uzuale și cotidiene, numerele naturale au multe proprietăți care sînt departe de a fi unanim cunoscute. Există o știință specială, teoria numerelor, care se ocupă cu studiul lor. Știința aceasta are o particularitate interesantă: problemele ei par simple și accesibile, iar rezultatele lor pot fi expuse persoanelor cu oarecare cultură. Însă rezolvarea problemelor și metodele prin care se ajunge la rezultate sînt cîteodată extrem de dificile și pe alocuri inaccesibile chiar celor mai buni matematicieni. Marele matematician german Gauss (1777—1855) a spus, pe bună dreptate, că aritmetica este regina matematicilor. Bineînțeles, el nu se referea la aritmetica elementară, ci la teoria numerelor, care mai este denumită și aritmetică superioară și a cărei dezvoltare a fost puternic influențată de lucrările lui Gauss.

Există o infinitate de numere naturale, dar nu există printre ele unul care să fie cel mai mare. Acest fapt ni se pare clar. În adevăr, oricît de mare ar fi numărul pe care îl luăm, dacă îi adăugăm o unitate, obținem un număr și mai mare. Caracterul infinit al șirului numerelor creează dificultăți considerabile la fundamentarea logică a aritmeticii.

În cartea de față nu ne ocupăm de fundamentele aritmeticii (axiomele și regulile ei cele mai simple).

Șirul numerelor naturale, adică al acelor numere care servesc pentru a număra obiectele, începe cu unu, nu cu zero. Zeroul se introduce împreună cu numerele negative pentru a face posibilă operația de scădere chiar și în cazurile cînd scăzătorul este egal sau mai mare decît descăzutul. Numerele întregi pozitive, cele întregi negative și zero formează sistemul numerelor întregi, ale cărui reguli fundamentale de efectuare a operațiilor le învățăm la începutul cursului de algebră din școala elementară. În această lucrare ne vom ocupa în special de proprietățile numerelor naturale. Vom recurge însă și la numerele negative și la zero acolo unde aceasta va putea simplifica expunerea.

Ce fel de chestiuni referitoare la numerele naturale vor fi studiate? În primul rînd, diferitele procedee pentru a le scrie și a le nota, dezvoltarea acestor procedee și relațiile dintre ele. Apoi se vor aborda problemele care apar la împărțirea numerelor întregi (divizibilitatea, cel mai mare divizor comun, descompunerea în factori primi etc.). În capitolele de la sfîrșitul cărții vor fi expuse unele proprietăți ale numerelor prime.

De teoria numerelor prime s-au ocupat unii dintre cei mai buni matematicieni ruși: Cebîșev, Zolotariov etc. În secolul al XX-lea, rezultate dintre cele mai importante în acest domeniu au fost obținute de matematicieni sovietici ca L. G. Șnirelman și, îndeosebi, academicianul I. M. Vinogradov. Despre aceste rezultate vom vorbi în ultimul capitol al cărții noastre.



CAPITOLUL I

SISTEMUL NOSTRU DE NUMERAȚIE



mul primitiv aproape că nu era pus în situația de a număra. „Unu”, „doi” și „mult” erau toate numerele cunoscute de el. Însă noi, oamenii contemporani, sîntem nevoiți să avem de-a face cu numere la fiecare pas. Trebuie să știm cum se numește și se scrie corect orice număr, oricît ar fi de mare. Dacă fiecare număr ar avea un nume și s-ar nota în scris printr-un semn special, nimeni nu ar fi în stare să țină minte toate aceste cuvinte și toate aceste simboluri. Cum rezolvăm deci această problemă? Ne vine în ajutor un sistem de notații rațional. Un ansamblu de cîteva denumiri și simboluri, care ne permite să scriem orice număr și să-l denumim, se numește sistem de numerație sau, mai simplu, numerație.

Numerația noastră obișnuită folosește pentru scrierea numerelor zece simboluri diferite. Nouă dintre ele servesc pentru notarea primelor nouă numere naturale (1, 2, 3, 4, 5, 6, 7, 8, 9), iar al zecelea nu desemnează nici un număr; el reprezintă „albitura” (intervalul) atunci cînd scriem numerele. Acest simbol se numește zero și se scrie 0.

Așadar, avem nouă simboluri pentru notarea primelor nouă numere și un al zecelea simbol — zeroul — „intervalul pozițional”. Aceste simboluri se numesc cifre.

Se pune întrebarea: cum putem scrie numerele cu ajutorul celor zece cifre? Să ne gîndim întîi cum am număra o cantitate mare de obiecte de același fel, de exemplu chibrituri. În acest scop am așeza întîi obiectele în grămezi de cîte zece, obținînd astfel un anumit număr de zeci (și, eventual, ne-ar mai rămîne cîteva

obiecte care nu au format o grămadă întreagă de zece). Mai departe ar trebui să numărăm grămezile de câte zece. Dacă am avea foarte multe asemenea grămezi, le-am grupa iarăși câte zece etc.

În felul acesta, ajungem la ideea fundamentală a sistemului nostru de numerație, la ideea unităților de diferite ordine. Zece unități formează o unitate superioară, de ordinul zecilor, cu alte cuvinte, zece unități de primul ordin formează o unitate de al doilea ordin. Zece unități de al doilea ordin formează o unitate de ordinul al treilea. În general, zece unități de un anumit ordin formează o unitate de ordinul următor.

Cu toată simplitatea aparentă, acest sistem de numerație a parcurs o cale foarte lungă în dezvoltarea sa istorică. La crearea lui au contribuit multe popoare.

Se pune o întrebare legitimă: de ce au început oamenii să grupeze obiectele câte zece și nu câte cinci sau câte douăsprezece? De ce o unitate de un anumit ordin este de zece ori mai mare decât o unitate de ordinul precedent și nu de opt sau de trei ori mai mare?

Sistemul de numerație cu baza zece a devenit foarte răspândit pentru motivul că omul dispune de „o mașină de calcul” naturală, legată de numărul zece: cele zece degete de la mâini.

Folosind cele zece simboluri principale și unele cuvinte de legătură, putem scrie orice număr; de exemplu „cincizeci și șapte” ar putea fi scris astfel: „5 unități de ordinul al doilea și 7 unități simple”. Acest mod de scriere este însă greoi. Este mai comod și mai scurt să renunțăm la cuvinte și să folosim simboluri (cifre). În adevăr, în acest caz, numărul „cincizeci și șapte” se scrie: 57. Aceste două cifre puse una lângă alta reprezintă suma a două numere: cea din dreapta (în exemplul nostru 7) dă numărul de unități de ordinul întâi (simple), iar cea din stînga (5) dă numărul de unități de ordinul al doilea (zeci). Dacă am scrie trei cifre una lângă alta, atunci cea din dreapta reprezintă unitățile de ordinul întâi, cea din mijloc unitățile de ordinul al doilea, iar cea din stînga unitățile de ordinul al treilea (sute). De exemplu 238 este suma dintre două sute, trei zeci și opt unități. În general, din două cifre scrise una lângă alta, cea din stînga reprezintă unități de zece ori mai mari decât unitățile reprezentate de cifra din dreapta. Nu numai cifra prezintă importanță, ci și locul sau poziția¹⁾ ei. De aceea, sistemul nostru de numerație este un sistem de numerație pozițional.

¹⁾ Cuvîntul poziție (așezare) vine de la latinescul „positio”.

Să scriem, conform numerației noastre, numărul „o sută doi”. Aici avem o unitate de ordinul al treilea (o sută) și două unități de ordinul întâi. Nu putem scrie „12”, deoarece altfel se scrie numărul „doisprezece”. Nu este comod nici să scriem „1 2”, lăsînd un interval pentru ordinul care lipsește; în felul acesta s-ar putea crede că am scris rărit numărul „doisprezece” sau pur și simplu două numere „unu” și „doi”. Cum să distingem, în scrierea noastră, numerele „doisprezece” și „o sută douăzeci”? Unde să lăsăm acum locul liber? Pentru înlăturarea acestor inconveniente a fost introdus „intervalul pozițional”, cifra zero. Ea se scrie în locul ordinului care lipsește. Datorită acesteia, numerele „doisprezece”, „o sută doi” și „o sută douăzeci” se scriu fiecare astfel: 12; 102; 120.

Numerația pozițională zecimală era cunoscută în India acum circa 1500 de ani (poate chiar înainte); în Europa ea a fost introdusă de arabi, care au cucerit Spania în secolul al VIII-lea e.n. Numerația arabă s-a răspîndit în toată Europa. Fiind mai simplă și mai comodă decât celelalte numerații, de care ne vom ocupa în capitolul următor, le-a luat curînd locul. Obiceiul de a da cifrelor noastre denumirea de arabe s-a păstrat pînă astăzi. De altfel, în timp de 1000 de ani toate cifrele, cu excepția lui 1 și a lui 9, s-au schimbat mult. Pentru comparație prezentăm cifrele noastre „arabe” și adevăratele cifre arabe:

Arabe	1	2	3	4	5	6	7	8	9	0
Europa, secolul X	1	Z	3	4	5	6	V	7	9	0
Europa, secolul XIV	1	2	3	X	7	6	7	8	9	0
Contemporane	1	2	3	4	5	6	7	8	9	0

Să spunem cîteva cuvinte despre denumirile numerelor. Denumirile primelor șase ordine (unități, zeci, sute, mii, zeci de mii, sute de mii) sînt foarte vechi și diferă de la un popor la altul. Studiul originii acestor denumiri îi revine lingvistului, nu matematicianului. Cuvîntul „milion” este de origine relativ recentă. În limba italiană „millione” este un augmentativ al lui „mille”, care înseamnă „mie”. Cuvîntul „milion” a fost inventat de cunos-

cutul explorator venețian Marco Polo (secolul al XIII-lea), căruia numerele obișnuite i s-au părut insuficiente pentru a relata extraordinara abundență de oameni și de bogății din îndepărtatul Imperiu al Cerului¹⁾. Astăzi denumim milioane, zeci de milioane și sute de milioane unitățile de ordinele al șaptelea, al optulea și al nouălea. O mie de milioane formează un bilion sau un miliard, iar mai departe, pentru a crea denumiri ale numerelor, aceleași în toată lumea, se folosesc numeralele din limba latină. Pentru a înțelege mai bine cum se construiesc denumirile acestor numere gigante, amintim că trei ordine formează o clasă. Astfel: unitățile simple, zecile și sutele formează prima clasă; miile, zecile de mii și sutele de mii, a doua clasă; milioanele, zecile de milioane, sutele de milioane, a treia clasă; bilioanele, zecile de bilioane, sutele de bilioane, a patra etc.

Pentru a denumi o unitate a unei anumite clase, începînd cu a patra, trebuie să micșorăm cu doi numărul de ordine al clasei, iar la numărul obținut (luînd denumirea latină) să adăugăm terminația „ilion“. Astfel, o unitate din clasa a cincea se numește „trilion“, pentru că $5-2=3$, iar 3 se numește în limba latină „tres“ (în cuvintele compuse însă „tres“ trece în „tri“). Să luăm o unitate din clasa a douăzeci și doua. Ne dăm ușor seama că aceasta va fi o unitate de ordinul al 64-lea (o unitate din clasa douăzeci și doua este precedată de 21 clase, adică de $21 \times 3 = 63$ ordine). Așadar, acest număr se scrie astfel:

1 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000 000

Ce nume să-i dăm? Scădem doi din numărul clasei: $22-2=20$; în limba latină, douăzeci se spune „viginti“, deci numărul nostru se va numi „vigintilion“.

Denumirile acestea sînt însă incomode. În primul rînd, nu toți știu latinește. În afară de aceasta, denumirile numerelor foarte mari sînt greu de pronunțat. Chiar un bun cunoscător al limbii latine nu va fi în stare să denumească, de exemplu, un număr format din cifra 1 urmată de cinci milioane de zerouri. De altfel, practic, este imposibil să scriem un astfel de număr.

De ce nu se schimbă atunci procedeul pentru denumirea și scrierea numerelor mari? Oare nu se pot introduce raționalizări? Desigur se poate și este chiar relativ ușor, dar nu este necesar. Numerele mari, de felul gigantului scris mai înainte, apar numai în culegerile de curiozități matematice și în unele capitole ale teoriei numerelor.

¹⁾ Așa se numea China în vechime.

Dați-mi voie, ne va întrerupe cititorul, dar în fizică, dar în astronomie? În adevăr, numerelor mari li se spune și numere „astronomice“!

Răbdare, cititorule! Ne vom ocupa acum și de numerele „astronomice“. Vom da însă înainte o tabelă a denumirilor unităților din ordinele superioare, nu atît pentru utilitatea lor (după cum vom vedea imediat, folosul lor nu este prea mare), cît pentru satisfacerea curiozității.

1 000 000 000 (unitate de ordinul 10 sau clasa 4) — bilion;
1 000 000 000 000 (unitate de ordinul 13 sau clasa 5) — trilion;
1 000 000 000 000 000 (unitate de ordinul 16 sau clasa 6) — cvadrilion;
1 000 000 000 000 000 000 (unitate de ordinul 19 sau clasa 7) — cvintilion.

Urmează apoi sextilionul, septilionul, octilionul, nonilionul, decilionul, undecilionul etc.

În unele țări, de exemplu în Franța, bilionul nu reprezintă o mie de milioane, ci un milion de milioane, adică o unitate de ordinul 13; trilionul este un milion de astfel de bilioane „mari“ (el corespunde cvintilionului nostru) etc. luînd clasele de cîte șase ordine, și nu de cîte trei. Aceasta simplifică întrucîtva denumirile numerelor mari.

Să trecem acum la „numerele astronomice“. Înainte de a „porni“ în spațiul interastral, să le căutăm pe Pămînt. Prin ce numere se exprimă, de exemplu, aria, volumul și masa globului terestru? Dacă vom cerceta orice manual de geografie, vom găsi:

aria globului terestru	509 000 000 km ²
volumul globului terestru	1 070 000 000 000 km ³
masa globului terestru	6 000 000 000 000 000 000 t.

Ultimul număr reprezintă șase unități de ordinul 22, adică șase sextilioane.

Toate aceste numere se caracterizează printr-o particularitate: ele sînt numere „rotunde“, care se termină cu zerouri. Bineînțeles, atît aria, cît și volumul Pămîntului nu se pot exprima decît aproximativ prin astfel de numere „rotunde“ de kilometri pătrați și cubi. „Rotunjimea“ este aici aparentă. În adevăr, toate măsurătorile geodezice de pe suprafața terestră sînt aproximative, deși se efectuează cu deosebită grijă; de aceea și numerele care exprimă aria și volumul globului terestru sînt aproximative.

Să cercetăm mai atent numărul 509 000 000 (cinci sute nouă milioane). Cele șase zerouri din dreapta nu înseamnă că lipsesc miile și ordinele inferioare. Aceste ordine ori ne sînt necunoscute, ori le omitem intenționat, deoarece nu avem nevoie de atîta precizie. Rotunjim rezultatul și spunem: numărul de kilometri pătrați

ai suprafeței terestre este format din cinci sute nouă milioane și un număr de mii, sute, zeci și unități, pe care nu le indicăm exact.

În viața de toate zilele, când numărăm obiecte în cantități foarte mari, de exemplu locuitorii unei țări sau globulele roșii din sângele omului, sau când măsurăm diferite mărimi, reușim să determinăm numai primele 3—4 cifre exacte ale rezultatului. Chiar în cele mai precise măsurători din fizica modernă, cu toate precauțiile luate, nu reușim să obținem mai mult de șapte, iar în cazuri foarte rare, opt cifre exacte. În cazul în care găsim un număr întreg mai mare de opt cifre, sîntem nevoiți să adăugăm la sfîrșit zerouri. Așadar, orice număr mare, pe care l-am întîlni în experiențe sau în practica zilnică, poate fi scris ca produsul dintre un număr de cel mult opt cifre (în majoritatea cazurilor de numai trei-patru cifre) și „o unitate cu zerouri”¹⁾. De exemplu, aria Pămîntului de 509 000 000 km² se poate scrie 509 × 1 000 000 sau 509 · 1 000 000. Numerele pînă la un miliard sînt relativ ușor de denumit și de scris. Deci toată problema se reduce la a scrie și a denumi în mod rațional numerele reprezentate printr-o unitate cu un număr mai mare de zerouri decît în cazul miliardului.

Aici ne vine în ajutor noțiunea de putere. Un număr reprezentat printr-o unitate urmată de zerouri este o putere a lui zece. De exemplu, o sută este puterea a doua a lui zece (100 = 10²), o mie este puterea a treia a lui zece (1 000 = 10³) etc. În general, un număr reprezentat printr-o unitate urmată de zerouri este o putere a lui zece, egală cu numărul de zerouri.

Generalizînd, avem

$$\underbrace{10\,000 \dots 000}_{p \text{ zerouri}} = 10^p.$$

Astfel, o unitate de ordinul al n -lea este puterea a $(n-1)$ -a a lui zece (de exemplu milionul, adică unitatea de ordinul al 7-lea, reprezintă 10⁶).

Aceste considerații ne permit să denumim și să scriem foarte scurt și comod toate numerele pe care le întîlnim în știință și în viața practică. Să considerăm, de exemplu, masa globului terestru. Iată numărul care o exprimă:

6 000 000 000 000 000 000 000 tone.

Acum îl putem scrie 6 · 10²¹ tone și citim: „șase ori zece la puterea douăzeci și unu tone”. Este și scurt și comod.

¹⁾ Așa se numește pe scurt un număr în care prima cifră este 1, iar toate celelalte sînt zerouri, cum ar fi 10, 100, 1 000, 10 000 000 etc.

Pentru a ne obișnui cu acest sistem de notații și denumiri, să analizăm cîteva exemple.

După primul război mondial (1914—1918), în mai multe țări, inclusiv Rusia, distrugerea economică a fost însoțită de o devalorizare a banilor. A fost necesar să se emită cantități imense de hîrtii cu valoare nominală din ce în ce mai mare. Acest fenomen, denumit inflație, a fost însoțit în Rusia de mai multe ori de o denominalizare, adică de emiterea unor bancnote cu valoare nominală relativ scăzută, specificîndu-se însă că o rublă din noua emisiune este egală cu o sută sau cu o mie de ruble din emisiunea precedentă. Aceste denominalizări au permis ca pe semnele monetare să nu se imprime numere prea mari: nu s-a mers dincolo de milioane. În schimb, în Germania, unde inflația nu a fost însoțită de denominalizare, existau bonuri și chiar timbre poștale cu o valoare nominală imensă: zeci și sute de miliarde de mărci! În fig. 1 sînt reproduse cîteva timbre poștale cu asemenea valori nominale „astro-nomice”. Valoarea nominală maximă a unui timbru poștal emis în Germania a fost de 50 miliarde, adică 5 · 10¹⁰ mărci; s-au emis bonuri cu valori și mai mari.



Fig. 1

Un exemplu clasic de număr gigant este răsplata pe care a cerut-o inventatorul jocului de șah dintr-o veche legendă orientală. Se spune că el a cerut pentru primul pătrățel al tablei de șah un bob de orez, pentru al doilea două, pentru al treilea patru etc.; pentru fiecare pătrățel următor de două ori mai mult decît pentru cel anterior. Această cerere, în aparență modestă, s-a dovedit a fi irealizabilă: toate orezăriile lumii nu erau în stare să cuprindă orezul cerut de vicleanul inventator. În adevăr, pentru primul pătrățel el ar fi trebuit să capete un bob, adică 2—1. Pentru primul și al doilea pătrățel, la un loc, i se cuveneau 1+2=3=2·2—1 boabe. Pentru primele trei pătrățele, urma să primească 1+2+4=7=2·2·2—1 boabe. Rezultă că pentru primele a pătrățele, trebuia să i se dea

$$\underbrace{2 \cdot 2 \dots 2}_{\text{de } a \text{ ori}} - 1 = 2^a - 1 \text{ boabe.}$$

Așadar, pentru cele 64 de pătrățele i se cuveneau inventatorului $2^{64} - 1$ boabe¹⁾. Numărul 2^{64} se calculează în modul cel mai ușor, folosind proprietatea de asociativitate a înmulțirii; în adevăr, 2^{64} este produsul a 64 de factori egali cu 2; putem forma trei grupe de câte 20 și o grupă de 4 factori egali cu 2; vom avea

$$2^{64} = 2^{20} \cdot 2^{20} \cdot 2^{20} \cdot 2^4.$$

Este ușor să calculăm $2^{10} = 1024$. Înmulțind 1024 cu el însuși, obținem $2^{20} = 1\,048\,576$. Prin urmare,

$$2^{64} = 1\,048\,576 \cdot 1\,048\,576 \cdot 1\,048\,576 \cdot 16.$$

Ne rămîne să efectuăm o înmulțire plicticoasă, însă ușoară. În cele din urmă obținem

$$2^{64} - 1 = 18\,446\,744\,073\,709\,551\,615.$$

Numărul acesta se citește: optsprezece cvintilioane, patru sute patruzeci și șase cvadrilioane, șapte sute patruzeci și patru trilioane, șaptezeci și trei bilioane, șapte sute nouă milioane, cinci sute cincizeci și una mii, șase sute cincisprezece. El este aproximativ egal cu $18 \cdot 10^{18}$ (se citește „optsprezece ori 10 la puterea optsprezece“).

Să ne amintim de cunoscuta problemă referitoare la numărul cel mai mare care se poate scrie cu trei cifre de 9.

Ca rezultat nu vom obține numărul banal 999, nici impresionantul 9^{99} sau 99^9 , ci gigantul „cu trei etaje“ 9^{99} . Cu ajutorul sistemului nostru de numerație, el se scrie aproximativ astfel: $4 \cdot 10^{369\,693\,099}$ (patru ori zece la puterea trei sute șasezeci și nouă milioane, șase sute nouăzeci și trei de mii, nouăzeci și nouă). Chiar sub forma aceasta prescurtată este greu să-l rostim!

Prin urmare

$$9^{99} \approx 4 \cdot 10^{369\,693\,099}$$

($\approx$ este semnul egalității aproximative).

În comparație cu acest număr imens, numerele „astronomice“ apar ca niște pitici jalnici. Să luăm, bunăoară, distanța pînă la cele mai îndepărtate galaxii accesibile observațiilor cu instrumen-

¹⁾ Cititorii familiarizați cu progresiile își vor da seama că numerele de boabe care revin fiecărui pătrățel formează o progresie geometrică cu rația 2, adică $\div 1, 2, 2^2, \dots, 2^{63}$. Suma termenilor acestei progresii este

$$\frac{2^{64} - 1}{2 - 1} = 2^{64} - 1.$$

tele moderne. Galaxiile sînt sisteme stelare grandioase formate din miliarde de stele; ele sînt situate la distanțe atît de mari, încît lumina lor ne parvine aproximativ într-un miliard de ani. Aceasta înseamnă că sînt situate la o distanță de aproape 10^{22} km sau $10^{22} \cdot 10^5 = 10^{27}$ cm (un kilometru are $100\,000 = 10^5$ cm). În fizică, obișnuim să exprimăm toate lungimile în centimetri; de aceea, am exprimat în centimetri și această distanță. Numărul 10^{27} este relativ ușor de denumit: în adevăr el este egal cu o unitate de ordinul a douăzeci și optulea sau o unitate din clasa a zecea. Scăzînd din zece doi, obținem opt (în legătură cu denumirile numerelor mari, v. p. 10). Prin urmare, denumirea unității noastre trebuie să provină de la cuvîntul latin „octo“ (opt), adică distanța pînă la galaxiile accesibile observațiilor cu telescoapele moderne este de un octilion de centimetri. Comparați aceasta cu numărul $4 \cdot 10^{369\,693\,099}$!

Să rezumăm. Am stabilit că pentru denumirea și scrierea numerelor folosim sistemul de numerație pozițional zecimal. El se numește pozițional, deoarece semnificația unei cifre depinde de poziția ei, adică de locul pe care îl ocupă printre celelalte cifre ale numărului respectiv; se numește și zecimal, pentru că dintre două cifre scrise una lîngă alta, cea din stînga reprezintă o unitate de zece ori mai mare decît cea din dreapta. Pentru denumirea și scrierea numerelor pînă la un miliard, acest sistem este foarte comod. Pentru scrierea numerelor foarte mari, el este incomod (ajungem la numere foarte „lungi“), iar pentru a le denumi este practic cu totul inutilizabil. Aceste inconveniente se pot înlătura dacă se utilizează noțiunea de *putere* a unui număr. Reprezentînd un număr sub forma produsului dintre un număr relativ mic și o putere a lui zece, scriem și denumim fără dificultate toate numerele întîlnite în știință și viața de toate zilele.





CAPITOLUL II

CUM NUMĂRAU STRĂMOȘII NOȘTRI?



u știm exact cum numărau oamenii și cum denu-
meau numerele înainte de apariția scrisului. În pri-
vința aceasta nu putem face decât ipoteze. Un lucru
este incontestabil: omenirea și-a însușit numerația
foarte încet. Pe primele trepte ale dezvoltării socie-
tății, oamenii se mărgineau la trei numere: „unu“, „doi“ și „mult“.
Au trecut, probabil, mii de ani înainte pentru ca acest „mult“ să
fi fost deplasat mai departe. În orice caz, în perioada când a
apărut scrierea, oamenii știau să numere destul de bine.

În urmă cu patru milenii, popoarele cele mai evolute (egip-
tenii, caldeenii) știau să scrie și să folosească numere întregi și
chiar fracții simple. Mai mult, pe atunci existau școli în care
se preda arta calculului.

În scrierile primitive nu se foloseau litere. Fiecare obiect
însușit sau neînsușit, fiecare acțiune erau redată prin mici
imagini. Treptat aceste imagini au fost simplificate; alături de
acestea, au apărut figuri care reprezentau diverse proprietăți ale
obiectelor, precum și simboluri pentru cuvintele corespunzătoare
prepozițiilor și conjuncțiilor noastre. Astfel a apărut scrierea de-
numită hieroglifică. În această scriere fiecărui simbol îi
corespunde un cuvânt întreg și nu un sunet, ca în scrierea noastră.
Pe atunci nu existau semne (cifre) speciale pentru scrierea nume-
relor, însă fiecareia dintre cuvintele „unu“, „doi“... „șaptespre-
zece“ etc. îi corespundea câte o hieroglifă determinată. Numărul
lor nu era chiar atât de mare, deoarece pe atunci oamenii nu

cunoșteau numerele mari. În unele țări (de exemplu în China și în
Japonia) scrierea hieroglifică s-a păstrat pînă în zilele noastre.

Iată hieroglifile japoneze care reprezintă numere:

1	2	3	4	5	6	7	
一	二	三	四	五	六	七	
8	9	10	11	12	13	20	22
八	九	十	十一	十二	十三	二十	二十二

Și mai complicate sînt hieroglifile chineze:

1	2	3	5
一	二	三	五

În cadrul scrierii hieroglifice nu putem vorbi despre un sistem
de numerație, pentru că nu există nici un sistem. Numai în Egiptul
antic s-a conturat ceva puțin asemănător cu numerația actuală.

Pe treapta următoare de dezvoltare au apărut literele care
reprezentau elementele sonore ale cuvintelor. În această perioadă,
oamenii știau să calculeze bine; în orice caz, ei cunoșteau miile
și zecile de mii. Atunci au apărut cifrele, adică semne sau
simboluri speciale pentru unele numere, astfel încît orice număr
(în limitele cunoscute) putea fi scris cu ajutorul acestor semne.
De obicei, serveau ca cifre aceleași litere ale alfabetului. Astfel
de numerații au existat la vechii evrei, la greci, la romani și la
slavi. Vom insista asupra numerației romane și a celei slave.

Cifrele romane sînt unanim cunoscute:

I	V	X	L	C	D	M
1	5	10	50	100	500	1000.

În fond, aceste simboluri nu sînt cifre, ci litere majuscule
latine. Ele au jucat însă rolul de cifre. Cu ajutorul lor romanii
puteau scrie orice număr pînă la un milion. Iată cum se proceda:
doi și trei se scriau respectiv II, III (adică două unități, trei
unități). Patru se scria astfel: IV, adică unitatea scrisă în stînga

„se scădea” din cinci. Dimpotrivă, unitățile scrise în dreapta lui cinci se adunau. Astfel, cinci, șase, șapte și opt se scriau:

V, VI, VII, VIII.

Mai departe a trebuit introdus semnul X. Nouă se scria astfel: IX (din zece se scade o unitate); zece, unsprezece etc. erau simbolizate prin

X, XI, XII, XIII, XIV.

Cincisprezece se obținea combinând simbolul pentru zece cu cel pentru cinci: XV. Douăzeci și treizeci se scriau cu ajutorul zecilor:

XX, XXX.

Pentru patruzeci și numerele următoare a trebuit introdus semnul L. De exemplu patruzeci și unu se scria astfel: XLI (zece se scade din cincizeci, iar unu se adaugă). Pentru nouăzeci se recurgea la semnul C al sutei, scriindu-se XC. Menționez că 49 și 99 nu se scriau XLIX și XCIX, ci IL și IC. O sută doi se scria CII, trei sute șaptezeci și patru CCCLXXIV etc. Un număr mare, să zicem 29 635, se scria astfel:

XXIX_mDCXXXV

(indicele *m* însemna „mii”; el reprezintă prima literă a cuvântului latinesc „mille” (mie).

Romanii aveau o numerație perfect elaborată, foarte economică (am văzut că erau necesare doar șapte cifre pentru a scrie numerele până la un milion), însă incomodă: numere relativ mici se scriau prin șiruri lungi și nu existau nici un fel de ușurări la calcule; calcule în scris nu se puteau face, astfel încât se calcula, de fapt, mintal.

Numerația slavă seamănă cu cea latină prin faptul că folosește și ea literele din alfabet pentru a scrie numerele. Nu este tot atât de economică, pentru că folosește 27 simboluri, însă scrierea este mult mai sistematică și permite să se simplifice considerabil efectuarea operațiilor. Spre deosebire de numerația romană, numerația slavă nu folosea literele majuscule, ci literele minuscule, prevăzute cu un semn special, tilda (˘) (care de altfel, se utiliza și în scrierea obișnuită, la prescurtarea cuvintelor).

Cifrele slave aveau următorul aspect:

ā	ḃ	ḥ	ā	ē	š	ž	h	ā
az	vedi	glagol	dobro	esti	zelo	zemlea	ije	fita
1	2	3	4	5	6	7	8	9
ī	ḱ	l	m	n	ž	o	p	č
i	kako	liudi	misle	naš	x	on	pokoi	cerv
10	20	30	40	50	60	70	80	90
ṛ	č	ṭ	ṽ	ḥ	ḥ	ṽ	ṽ	č
rî	slovo	tverdo	uk	fert	ha	psi	o	ŭ
100	200	300	400	500	600	700	800	900

Numerele unsprezece, doisprezece, ... se scriau respectiv āī, āī, ...; douăzeci și unu, douăzeci și doi, ... se scriau ḱā, ḱā, ... etc. Tilda se puneă numai pe una dintre cifre. Ordinea cifrelor la scrierea unui număr era aceeași ca și în pronunțarea lui. De exemplu, în limba rusă se spune pentru cincisprezece „peatinadșati” (în slavă era peatinadeseati), rostind întâi cifra unităților și apoi pe a zecilor. Slavii scriau astfel: ēī, adică puneau întâi un cinci, iar după aceea un zece. Dimpotrivă, în numărul „dvadșati tri” (douăzeci și trei), în limba rusă se enunță întâi zecile, apoi unitățile. La slavi acest lucru se reflectă întocmai în scriere: ei scriau ḱr. Locul cifrei, poziția ei în număr nu avea nici o importanță.

Cu ajutorul acestor simboluri se scriau ușor numerele mari. De exemplu numărul 29 946 se scria astfel ḱā ŭms (simbolul * însemna mii). Cu ajutorul repetării semnelor * se puteau

scrie numere foarte mari. Iată, de exemplu, cum se scria numărul 20 178 073: 𐎶𐎵 𐎶𐎵𐎶𐎵 𐎶𐎵 . Se vede ușor că acest sistem de

scriere permite efectuarea operațiilor „pe coloane”, aproape în același fel cum procedăm astăzi.

Numerația pozițională a apărut, după toate probabilitățile, în vechiul Babilon. Ea a luat acolo o formă aparte, de care merită să ne ocupăm mai amănunțit. De la babilonieni numerația pozițională a trecut la indieni.

La indieni, ca și la multe alte popoare antice, primii matematicieni au fost preoții. Ei aveau grijă de calendar și țineau socoteala sărbătorilor, observau corpurile cerești și trebuiau să fie capabili să prevadă diversele fenomene cerești (de exemplu, eclipsele). Pentru aceasta, erau necesare anumite cunoștințe de matematică. Din legătura care a existat în timpurile străvechi între matematică și religie, s-a păstrat o rămășiță curioasă: superstițiile relative la numere. Și în zilele noastre există oameni care cred că numărul 3 aduce noroc, pe când 13 este purtător de ghinion („duzina diavolului”).

Cu trei mii de ani în urmă, indienii foloseau o numerație bine elaborată, deși în documentele aceluia timp nu figurează numere mai mari de 100 000. În operele indiene ulterioare se întâlnesc numere considerabil mai mari, până la o sută de cvadrilioane (10^{17}). Într-o legendă despre Buda (legenda nu are nici 1 000 de ani), se spune că el știa denumirile numerelor până la 10^{54} . De altfel se pare că indienii nu aveau o idee clară despre infinitatea șirului numerelor naturale, crezând că există un număr „cel mai mare”, cunoscut numai de zei. Demonstrația infinității șirului numerelor este un merit al învățaților elini.

După cum am spus, matematica babiloniană prezintă un deosebit interes. Numerația babiloniană a fost constituită cu aproape patru mii de ani în urmă, a existat aproape un mileniu și jumătate (din secolele XVIII—III î.e.n.) și a fost larg răspândită în tot Orientul Apropiat. Ea a influențat matematica chineză, indiană și greacă și, după cum vom vedea, a lăsat urme chiar în știința contemporană.

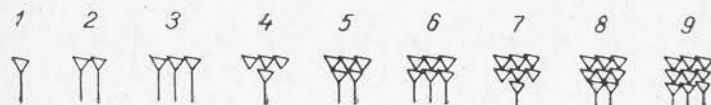
Babilonienii scriau cu bețișoare pe plăci de humă moale și întăreau apoi prin ardere „manuscrisele”. Ei obțineau astfel „documente” din cărămidă durabilă, care s-au păstrat în parte până în zilele noastre; aceste documente se găsesc frecvent în săpăturile

arheologice efectuate în Mesopotamia (Irakul actual). De aceea, istoria Babilonului și în particular matematica babiloniană au putut fi destul de bine studiate.

La începutul secolului al XVIII-lea î.e.n., s-a produs contopirea a două popoare: sumerienii și acadienii. Fiecare dintre aceste popoare avea un comerț destul de bine dezvoltat, unități de greutate și unități bănești. Fără îndoială, comerțul de atunci nu necesita multe calcule, astfel că nici unul dintre aceste popoare nu avea o numerație bine elaborată. Unitatea de masă a sumerienilor era „mina” (aproximativ 0,5 kg). Unitatea bănească era o mină de argint. La acadieni unitatea principală era un „șekel”, de aproximativ șasezeci de ori mai mică decât mina (bineînțeles, aproximația se datorește cântărelor primitive ale timpului care nu sesizau diferențe mici). După contopirea acestor două popoare, „au circulat” ambele sisteme de unități; mina și șekelul se foloseau așa cum folosim astăzi kilogramul și gramul. În circulația bănească, mina și șekelul jucau rolul pe care-l au rubla și copeica astăzi în U.R.S.S., cu singura deosebire că unitatea mai mare era egală cu 60 de unități mici și nu cu o sută. Comerțul și economia se dezvoltau, circulația bănească creștea. După cum noi avem nevoie de tone, în afară de grame și de kilograme, tot astfel a apărut și acolo o unitate de greutate mai mare, „talantul”. Firește, dat fiind că divizarea în „șasezeci” ajunsese uzuală în calculele economice, noua unitate s-a ales de șasezeci de ori mai mare decât cea existentă: un talant era egal cu șasezeci de mine.

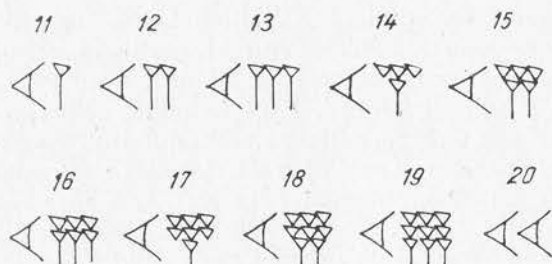
Cum scriau babilonienii numerele? Ei scriau cu bețișoare pe lutul moale, astfel că principalul element grafic era un cui mic de forma 𐎶 sau 𐎵 . Pentru a reprezenta unitatea, se scria

un singur cui, așezat vertical 𐎶 . Scrierea numerelor de la unu până la nouă este naturală și ușor de înțeles:



Fiecare număr până la 9 inclusiv era reprezentat prin numărul corespunzător de cuie, așezate atât de rațional, încât la lectură ele nu trebuiau numărate: numărul lor era evident.

Pentru zece exista semnul special . Scrierea numerelor de la unsprezece pînă la douăzeci este de asemenea ușor de înțeles :



Vedem că aceste semne sînt foarte clare. Acum, cititorul va fi în stare, fără nici o dificultate, să scrie orice număr mai mic decît o sută. De exemplu, numerele 37 și 54 se scriu astfel :



Numerele din a opta și a noua grupă de zece au o scriere destul de greoaie ; însă de ele nu era nevoie. Babilonienii nu erau de loc puși în situația de a scrie un număr mai mare decît 59, deoarece dispuneau de cele trei unități.

Inițial, minele se scriu cu simboluri mai mari decît șekeli. De exemplu, 20 mine și 37 șekeli se scria astfel :



Ulterior, toate semnele au ajuns să aibă aceeași mărime și numai poziția unui simbol arăta ce unități reprezintă. De exemplu, 2 talanți, 13 mine și 41 șekeli se scria astfel :



Dacă se lucra numai cu o singură unitate de măsură, nici aceasta nu era notată în vreun fel. Textul care însoțea numerele permitea imediat să se vadă despre ce fel de unități de măsură era vorba.

Pe la începutul secolului al XVIII-lea î.e.n. au apărut texte pur matematice : tabele pentru ușurarea calculelor, reguli pentru rezolvarea unor probleme etc. Astronomia ajunsese la un înalt grad de dezvoltare. În legătură cu aceasta era necesar, în primul rînd, să se opereze din ce în ce mai frecvent cu numere mari, iar în al doilea rînd, să se treacă de la numere concrete la numere abstracte. În loc de a imagina o numerație nouă, a început să fie folosită pentru noile scopuri numerația elaborată înainte. Notăția



nu mai însemna neapărat 1 talant, 23 mine și 15 șekeli, ci în același mod se scria numărul abstract format dintr-o unitate de ordinul al treilea, 23 de unități de ordinul al doilea și 15 unități de ordinul întâi, unitățile fiecărui ordin fiind de 60 de ori mai mari decît unitățile ordinului precedent. Scrierea

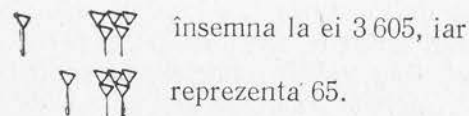


înseamnă, în sistemul nostru, $1 \cdot 60^2 + 23 \cdot 60 + 15$, adică 4995. Analog se scriu numerele cu patru, cinci și, în general, cu mai multe cifre. De exemplu



înseamnă $2 \cdot 60^3 + 11 \cdot 60^2 + 4 \cdot 60 + 43$, adică 471883. Numărul cel mai mare, care se întâlnește în „manuscrisele“ babiloniene, este egal cu $60^8 + 10 \cdot 60^7$. Numerația babiloniană era un sistem perfect elaborat cu baza 60, adică o numerație sexagesimală.

Cum scriau babilonienii cifra zero ? De exemplu, cum scriau ei numărul 3605, egal cu $1 \cdot 60^2 + 5$, adică numărul care conține o unitate de ordinul al treilea, cinci unități de ordinul întâi și nici o unitate de ordinul al doilea ? Timp de secole ei nu au folosit de loc semnul de despărțire. Dacă era necesar, se lăsa între cifre un interval mai larg :

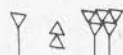


însemna la ei 3605, iar

reprezenta 65.

Scrierea cuneiformă este însă foarte incomodă pentru aprecierea intervalelor dintre cifre, iar faptul că se copia totul manual, ducea la erori frecvente. Semnul de despărțire era indispensabil și, în consecință, el a apărut. Incepând cu o anumită perioadă (nu se poate stabili data exactă), pe cărămizile babiloniene se găsește simbolul , corespunzător zeroului nostru.

De exemplu, 3 605 se scrie cu ajutorul zeroului



iar 65 astfel:



Ele nu mai pot fi confundate.

Introducând însă „intervalul pozițional” în interiorul numerelor, babilonienii nu au mers până acolo încât să-l pună și la sfârșitul lor. Chiar până la decăderea culturii babiloniene, numerele

„unu”, „șasezeci”, „trei mii, șase sute” se scriau la fel: . Babilonienilor nu le-a venit ideea de a nota pe 60 astfel:

 . Abia indienii, care au preluat de la ei numerația pozițională, au învățat să utilizeze corect simbolul zero și, introducând baza zece în locul lui șasezeci, au dat numerației forma ei actuală.

Sistemul de numerație babilonian (sexagesimal) s-a menținut până în prezent la măsurarea unghiurilor și a timpului. A șasea parte dintr-un cerc se împarte în 60 de grade, gradul în 60 de minute, minutul în 60 de secunde. Tot astfel, ora se împarte în 60 de minute, iar minutul în 60 de secunde, după cum talantul se împărțea în 60 de mine, iar mina în 60 de șekeli. Cu acest prilej vom spune câteva cuvinte despre originea termenilor „minut” și „secundă”. Minut este traducerea cuvântului latin „minuta” care înseamnă „mic”, iar secunda a cuvântului „secunda”, care înseamnă „a doua”. Minutele erau „partes minutae primae”, adică „primele părți mici”, iar secunde erau „partes minutae secundae”, adică „părțile mici secunde” ale gradului sau ale orei.

Să rezumăm cele expuse în acest capitol. Omenirea și-a însușit numerația încet. I-au trebuit multe secole pentru a trece de la numerele „unu”, „doi” și „mult” la zeci și la sute. Chiar după

ce au învățat să scrie, oamenii nu au avut, mult timp, o numerație elaborată și au notat numerele cu ajutorul unor hieroglife.

La vechii evrei, iar de la aceștia la greci, la romani și la slavi a apărut numerația cu ajutorul literelor alfabetului. Această numerație a dăinuit aproximativ 2000 de ani și era suficientă pentru cerințele practicii.

Cu aproape 4000 de ani în urmă, a apărut în Babilon numerația pozițională. În India ea a luat forma numerației pozitoriale zecimale, cu folosirea „intervalului pozițional” — zeroul. De la indieni acest sistem de scriere a numerelor a trecut la arabi, care au devenit în secolele VIII—IX unul dintre cele mai civilizate popoare ale lumii. Europeanii au preluat acest sistem de la arabi (de unde și denumirea de cifre „arabe”).

În prezent, numerația pozițională zecimală este pe deplin suficientă pentru cerințele științei și ale practicii. Când trebuie să scriem numere foarte mari, este comod să recurgem la exprimarea prin puteri ale lui zece.





CAPITOLUL III

DE CE A NUMĂRAT ARHIMEDE FIRELE DE NISIP ȘI CUM LE-A NUMĂRAT ?



n secolul al III-lea î.e.n. a trăit în insula Sicilia un matematician cu un talent excepțional. Și astăzi, după aproape două milenii de la moartea lui, orice elev îi cunoaște numele. Este vorba de Arhimede.

Remarcabil geometru, mecanician, fizician și inginer militar, el ne-a lăsat, printre numeroasele sale creații, un admirabil tratat de aritmetică. Titlul lui este „Psammit sau Calculul nisipului într-un spațiu egal cu sfera stelelor fixe“.

Arhimede a fost cel dintâi care a arătat în mod convingător că pentru orice cantitate de obiecte, oricât ar fi ea de mare, se poate găsi un număr care să-i corespundă; pentru orice număr se poate indica locul lui în șirul numerelor deja cunoscute; se pot construi numere și mai mari și se pot da denumiri tuturor acestor numere. Cu alte cuvinte, el a construit un sistem de numerație științific.

Arhimede a demonstrat că dacă se presupune o sferă egală cu sfera stelelor fixe după Aristarh¹⁾, umplută cu nisip, se vor putea găsi și în acest caz numere care să fie mai mari decât numărul firelor de nisip din această sferă. Pentru a elimina dinainte orice obiecții posibile împotriva demonstrației acestei propoziții, Arhimede a admis că raza sferei stelelor fixe este

¹⁾ Arhimede s-a bazat pe concepțiile eminentului astronom grec Aristarh din Samos (sfârșitul sec. al IV-lea — prima jumătate a sec. al III-lea î.e.n.), după concepția căruia Soarele este imobil și situat în centrul sferei stelelor fixe, iar Pământul se rotește pe un cerc în al cărui centru se află Soarele.

egală cu o miriadă, adică este de 10 000 de ori mai mare decât distanța de la Pământ la Soare, considerind că această distanță este de o miriadă de miriade de stadii, adică, în scrierea actuală, de $150 \cdot 10^7$ km¹⁾. Aceasta întrece de zece ori distanța medie de la Pământ la Soare, pentru care măsurătorile actuale dau aproximativ $150 \cdot 10^6$ km. Așadar, raza sferei stelelor fixe era egală după Arhimede cu $15 \cdot 10^{12}$ km, ceea ce depășea cu mult chiar raza sferei stelelor fixe după Aristarh. Aceasta este aproximativ o treime din distanța efectivă pînă la steaua cea mai apropiată de noi. Deci, valoarea adoptată de Arhimede pentru raza sferei stelelor fixe este de circa 650 milioane de ori mai mică decât distanța pînă la galaxiile accesibile observațiilor cu instrumentele noastre moderne.

Avînd aceste date, nu este greu să calculăm volumul „sferei stelelor fixe“. El este egal cu

$$\frac{4}{3} \pi R^3 \approx 4 \cdot 15^3 \cdot 10^{36} = 135 \cdot 10^{38} \text{ km}^3 \text{ } ^{2)}$$

Mai rămîne să calculăm cîte fire de nisip pot încăpea în acest volum. Arhimede considera că într-o sămînță de mac încap o miriadă de fire de nisip, adică 10 000 fire (cu alte cuvinte, el a considerat un nisip foarte fin, ca o pulbere ușoară). După socoteala sa, diametrul unei semințe de mac era egal cu a patruzecea parte dintr-un țol³⁾, adică după unitățile noastre cu $1/2$ mm.

Dacă vom admite, pentru simplitate, că sămînța are forma unui cub, vom vedea că un milimetru cub conține opt semințe de mac sau 80 000 fire de nisip; un metru cub conține de 10^9 (de un bilion) ori mai mult, adică $8 \cdot 10^{13}$ fire, iar un kilometru cub conține de încă 10^9 ori mai mult, adică $8 \cdot 10^{13} \cdot 10^9 = 8 \cdot 10^{22}$ fire de nisip. Rămîne să înmulțim numărul de kilometri cubi din „sfera stelelor fixe“, adică $135 \cdot 10^{38}$, cu numărul de fire de nisip dintr-un kilometru cub. Acest calcul ne dă aproximativ 10^{63} fire de nisip — un număr imens chiar după reprezentările noastre actuale.

¹⁾ Stadia elină era egală cu aproximativ 150 m. De la cuvîntul „stadie“ provine termenul „stadion“; inițial, acesta era o cărare împărțită în stadii, pe care se întreceau alergătorii. Cuvîntul „miriadă“ înseamnă zece mii. Limba greacă nu dispunea de cuvinte pentru desemnarea numerelor mai mari de 10 000.

²⁾ Pentru simplificare, am considerat $\pi = 3$. Această aproximație nu influențează esența rezultatului.

³⁾ Țolul vechi grecesc măsura aproximativ 2 cm.

Am rezolvat fără dificultate problema lui Arhimede. Pe timpul lui Arhimede însă nu existau denumiri pentru numerele mai mari de zece mii, nu exista sistemul de numerație zecimal, nu se cunoșteau exponenții, nu existau reguli de operații. Meritul lui Arhimede este tocmai acela de a fi imaginat cum trebuie denumite numerele mari și cum să se efectueze calculele cu ele (în calcule el a folosit numai proprietățile progresiilor aritmetice și geometrice, cunoscute pe atunci). Calculul lui Arhimede este foarte interesant, însă nu avem posibilitatea să ne ocupăm de el în mica noastră carte¹⁾. Ne vom ocupa numai de sistemul de numerație al lui Arhimede.

Pentru primele zece mii, adică pentru prima miriadă, Arhimede a folosit numerele eline care existau în vremea sa. Mai departe, el a denumit numerele pînă la miriada de miriade la fel cum denumim noi numerele pînă la o mie de mii. Astfel, numărul 85 643 911 va fi, după Arhimede: „opt mii cinci sute șasezeci și patru de miriade, trei mii nouă sute unsprezece“. Toate numerele de la unu pînă la miriada de miriade le-a numit „primele numere“. El a denumit unitatea simplă „unitatea primelor numere“, iar miriada de miriade de unități ale primelor numere „unitatea numerelor secunde“. Așadar, o „unitate a numerelor secunde“ este egală cu 10^8 . În acest fel este ușor de găsit denumirea numerelor pînă la miriada de miriade de „unități ale numerelor secunde“, adică în scrierea noastră, pînă la 10^{16} . Acest număr era numit de Arhimede „unitate a numerelor terțe“ etc. Prin urmare, este vorba de un sistem de numerație pozițional cu baza 10^8 , în care s-au elaborat numai denumirile numerelor, nu și scrierea lor (care nu-l interesa pe Arhimede pentru rezolvarea problemei sale). La Arhimede, fiecare unitate de un ordin oarecare era de 10^8 ori mai mare decît unitatea de ordinul precedent.

În felul acesta se poate ajunge pînă la unitatea numerelor de ordinul miriadei de miriade. Se vede ușor că o unitate a numerelor de ordinul n va fi egală cu $10^{8(n-1)}$. [de exemplu unitatea numerelor de ordinul zece este $10^{8(10-1)} = 10^{72}$; o unitate a numerelor de ordinul o sută douăzeci și patru este $10^{8(24-1)} = 10^{984}$ etc.]. Numerația poate fi continuată pînă la o miriadă de miriade de numere de ordinul miriadei de miriade, adică pînă la $10^8 \cdot 10^{8(100\,000\,000-1)} = 10^{8 \cdot 10^8}$. Aceste numere ale lui Arhimede

¹⁾ Cei care se interesează de această problemă pot citi „Psammit“ care, începînd din anul 1824, a fost tradusă de mai multe ori în limba rusă. Ultima ediție: „Исчисление песчинок“ (Псаммит), М.-Л., 1932, traducere de G. N. Попов.

erau pe deplin suficiente pentru rezolvarea problemei sale. În adevăr, am văzut că soluția este $10^{63} = 10^7 \cdot 10^{8(8-1)}$, adică o mie de miriade de unități ale numerelor de ordinul opt.

Însă Arhimede nu s-a oprit aici. Așa cum noi introducem, pe lîngă unitățile de diferite ordine, unități ale diferitelor clase, tot astfel a introdus și el numere de diferite perioade. Arhimede a denumit toate numerele pînă la $10^8 \cdot 10^8$ „numere din prima perioadă“. O miriadă de miriade de numere de ordinul miriadei de miriade se numea în sistemul lui „unitatea primelor numere din perioada a doua“. Apoi urmau numerele secunde, terțe etc. pînă la cele de ordinul miriadei de miriade din perioada a doua. O miriadă de miriade de numere de ordinul miriadei de miriade din perioada a doua ($10^2 \cdot 8 \cdot 10^8$), formează o unitate a primelor numere din perioada a treia. Unitatea primelor numere din perioada a patra este numărul $10^{3 \cdot 8 \cdot 10^8}$. În general, o unitate a primelor numere din perioada a n -a este $10^{(n-1) \cdot 8 \cdot 10^8}$, iar o unitate a numerelor de ordinul m din perioada a n -a este $10^{(n-1) \cdot 8 \cdot 10^8 + m \cdot 8 - m}$. Astfel Arhimede a ajuns pînă la miriada de miriade a numerelor de ordinul miriadei de miriade din perioada de ordinul miriadei de miriade, adică pînă la numărul $10^{8 \cdot 10^{16}}$. El s-a oprit aici. Nu este greu însă să-i continuăm drumul. După perioade, putem introduce cicluri sau perioade de ordinul al doilea etc.

Sistemul de numerație a lui Arhimede se reprezintă comod sub forma următoarei tabele:

Perioada întâi — de la 1 pînă la $10^8 \cdot 10^8 - 1$ conține:	
Primele numere — de la 1 pînă la $10^8 - 1$	
Numerele secunde — de la 10^8 pînă la $10^{16} - 1$	
Numerele de ordinul m — de la $10^{(m-1) \cdot 8}$ pînă la $10^{8m} - 1$	
Numerele de ordinul miriadei de miriade — de la $10^{8(10^8-1)}$ pînă la $10^{8 \cdot 10^8} - 1$.	
Perioada a doua — de la $10^8 \cdot 10^8$ pînă la $10^{2 \cdot 8 \cdot 10^8} - 1$	
Primele numere — de la $10^8 \cdot 10^8$ pînă la $10^{8 \cdot (10^8+1)} - 1$	
Perioada a treia — de la $10^{2 \cdot 8 \cdot 10^8}$ pînă la $10^{3 \cdot 8 \cdot 10^8} - 1$	
Perioada a N -a, de la $10^{(N-1) \cdot 8 \cdot 10^8}$ pînă la $10^{8N \cdot 10^8} - 1$.	
Primele numere — de la $10^{(N-1) \cdot 8 \cdot 10^8}$ pînă la $10^{(N-1) \cdot 8 \cdot (10^8+1)} - 1$	

Numerale de ordinul m — de la $10^{(N-1) \cdot 8 \cdot 10^8 + 8m - 8}$
 pînă la $10^{(N-1) \cdot 8 \cdot 10^8 + 8m - 1}$

Numerale de ordinul miriadei de miriade — de la
 $10^{8 \cdot N \cdot 10^8 - 8}$ pînă la $10^{8 \cdot N \cdot 10^8 - 1}$

Perioada de ordinul miriadei de miriade — de la $10^{(10^8-1) \cdot 8 \cdot 10^8}$
 pînă la $10^{8 \cdot 10^{16}} - 1$.

Pentru a ne orienta mai bine în numerația arhimediană și pentru a-i aprecia meritele la justa valoare, să vedem cum putem denumi cu ajutorul ei numerele gigantice de care ne-am ocupat în capitolul I.

După cum s-a arătat la p. 14, inventatorul jocului de șah a cerut 18 446 744 073 709 551 615 boabe.

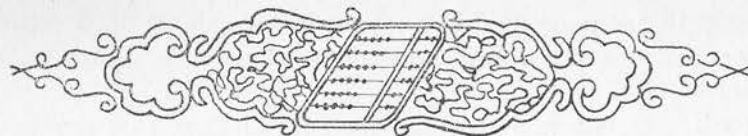
Să descompunem acest număr în „ordine arhimediene“, adică în grupe de cîte opt cifre. Rezultă

1844 6744 0737 0955 1615.

Evident, aici avem o mie opt sute patruzeci și patru de unități ale numerelor terțe, șase mii șapte sute patruzeci și patru de miriade, șapte sute treizeci și șapte de unități de numere secunde, nouă sute cincizeci și cinci miriade, o mie șase sute cincisprezece unități de prime numere. Această denumire este ceva mai lungă decît a noastră (optsprezece cvintilioane... etc., v. p. 14).

Pentru numărul 9^{9^9} , ar fi fost de ajuns numerele din prima perioadă. Dacă trecem însă la numărul $10^{10^{10}}$; el va fi egal cu o unitate a numerelor de ordinul cinci mii de miriade și unu din perioada a treisprezecea.

Iată ce instrument de calcul comod a creat Arhimede în urmă cu două mii de ani!



CAPITOLUL IV

NU CITE ZECE, CI CITE CINCI SAU CITE DOUĂSPREZECE



e pare că în stadiul actual de dezvoltare a științei nu putem imagina un sistem de numerație care să fie mai comod decît cel pozițional. Însă, ca bază a unui sistem de numerație pozițional se pot lua diferite numere.

La rezolvarea unor probleme se dovedesc a fi comode sisteme de numerație poziționale cu anumite baze. Poate că unele sisteme, de exemplu cel cu baza 12, s-ar arăta în ansamblul lor întrucîtva superioare celui zecimal. Însă obișnuința de a număra din zece în zece este atît de mare, iar trecerea obligatorie la noul sistem de numerație ar provoca o perturbare a tuturor deprinderilor și cheltuieli materiale atît de mari, încît este puțin probabil ca o astfel de reformă să poată fi considerată oportună.

Există totuși un sistem de numerație specific, ale cărui avantaje față de cel zecimal în unele probleme și dezavantaje în altele sînt atît de evidente, încît merită să-l analizăm mai amănunțit. Este vorba de sistemul binar, adică de sistemul cu baza 2. Îi vom consacra capitolul următor. În capitolul de față ne vom ocupa de sistemele poziționale nezecimale, în general, și vom învăța să trecem de la unul dintre aceste sisteme la altul.

În afara numerației cu baza zece, este destul de răspîndită în viața de toate zilele numerația cu baza 5. Numerația cu baza 5 este obișnuită în China, grupurile de cîte 5 îmbinîndu-se în perechi; se obține astfel un sistem de numerație original, în care orice unitate de ordin par este de cinci ori mai mare decît cea

precedentă, iar orice unitate de ordin impar este de două ori mai mare decât cea precedentă. Instrumentul de calcul este sciotul chinezesc (fig. 2).

Fără a insista mai mult asupra acestui sistem de numerație complicat (cu ambele mâini), să analizăm sistemul pozițional cu baza 5. În acest sistem se folosesc pentru scrierea tuturor numerelor numai cinci simboluri (cifre) și anume: simboluri pentru numerele „unu”, „doi”, „trei”, „patru” și intervalul pozițional — semnul zero. Pentru notarea primelor patru numere și a lui zero, putem folosi eventual și cifrele noastre: **1, 2, 3, 4, 0**, însă tipărite cu caractere grase.

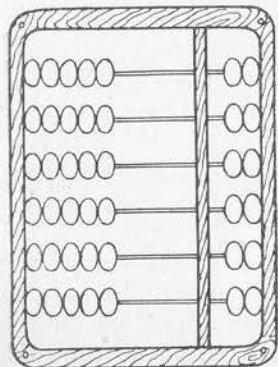


Fig. 2

Numărul „cinci” este o unitate de ordinul al doilea și va trebui scris astfel: **10** (cum scriem noi zece), punind un zero în locul unităților simple care lipsesc.

Să scriem în sistemul cu baza 5 numărul 387 (trei sute optzeci și șapte; caracterele obișnuite, subțiri, reprezintă notația uzuală, zecimală). În primul rând să stabilim câte grupe de cinci (unități de ordinul al doilea) cuprinde numărul nostru și câte unități simple. Pentru a ne da seama de aceasta, împărțim 387 prin cinci. Cîțul ne va da numărul de „cinciuri”, iar restul va fi numărul de unități simple:

$$\begin{array}{r} 387 : 5 = 77 \\ - 35 \\ \hline 37 \\ - 35 \\ \hline 2 \end{array}$$

Așadar, numărul nostru cuprinde 2 unități simple și 77 unități de ordinul al doilea. Însă fiecare cinci unități de ordinul al doilea formează o unitate de ordinul al treilea; evident, în șaptezeci și șapte de unități de ordinul al doilea este conținut un anumit

număr de unități de ordinul al treilea. Pentru a-l găsi repetăm operația de împărțire; împărțim 77 prin 5:

$$\begin{array}{r} 77 : 5 = 15 \\ - 5 \\ \hline 27 \\ - 25 \\ \hline 2 \end{array}$$

Restul 2 ne dă numărul de unități de ordinul al doilea, iar cîțul reprezintă numărul de unități de ordinul al treilea. Căutăm acum numărul de unități de ordinul al patrulea conținute în 15 unități de ordinul al treilea. El va fi egal cu

$$15 : 5 = 3.$$

Prin urmare, cincisprezece unități de ordinul al treilea sînt formate din trei unități de ordinul al patrulea. Lipsa restului ne arată că nu avem unități „libere” de ordinul al treilea. Cît privește cele trei unități de ordinul al patrulea, este clar că ele nu pot conține unități de ordin superior. Prin urmare, numărul 387 este format din trei unități de ordinul al patrulea, nu conține unități de ordinul al treilea, conține două unități de ordinul al doilea și două unități de ordinul întîi, adică îl putem scrie **3022**.

Toate operațiile pot fi grupate în modul următor:

$$\begin{array}{r} 387 \\ - 35 \\ \hline 37 \\ - 35 \\ \hline 2 \end{array} \quad \begin{array}{r} 5 \\ - 77 \\ \hline 5 \\ - 27 \\ \hline 25 \\ - 25 \\ \hline 2 \end{array} \quad \begin{array}{r} 5 \\ - 15 \\ \hline 15 \\ - 15 \\ \hline 0 \end{array} \quad \begin{array}{r} 5 \\ - 3 \\ \hline 2 \end{array}$$

Numerele tipărite cu caractere grase (resturile și ultimul cît) trebuie scrise în ordine inversă, pentru a obține numărul căutat în sistemul cu baza 5.

Să rezolvăm problema inversă. Fie dat un număr în sistemul cu baza cinci, de exemplu **2341**, și să căutăm expresia lui în sistemul zecimal.

Să ne gândim ce reprezintă fiecare dintre cifrele acestui număr. Unitatea din dreapta înseamnă, pur și simplu, 1. Cifra 4 din locul al doilea reprezintă patru „cinciuri“, adică $4 \cdot 5$; cifra 3 care urmează reprezintă trei „cinciuri luate de câte cinci ori“, adică $3 \cdot 5^2$; în sfârșit, cifra 2 din extrema stângă reprezintă $2 \cdot 5^3$. Prin urmare:

$$2341 = 2 \cdot 5^3 + 3 \cdot 5^2 + 4 \cdot 5 + 1 = 346.$$

Menționăm că și un număr scris în sistemul zecimal, de exemplu 3208, poate fi scris într-o formă analogă: $3 \cdot 10^3 + 2 \cdot 10^2 + 0 \cdot 10 + 8$ (în termenul al treilea al acestei expresii factorul „zero“ este un număr întreg, însă nu natural).

În general, dacă am luat ca bază a sistemului de numerație numărul m , atunci $abcdk$ ¹⁾ înseamnă

$$a \cdot m^4 + b \cdot m^3 + c \cdot m^2 + d \cdot m + k.$$

În viața de toate zilele s-au păstrat unele rămășițe ale numerației cu duzinile. Piciorul englezesc (ca și cel rusesc) se împart în 12 țoli. Anumite mărfuri se ambalează în duzini, iar pentru o duzină de duzini există în comerț o denumire specială: un gros. Trebuie menționat că sistemul de numerație cu baza 12 este, în unele privințe, superior celui zecimal, deoarece doisprezece are patru divizori întregi (în afară de 1 și de 12 însuși: aceștia sînt 2, 3, 4, 6), pe cînd zece nu are decît doi (2 și 5). De aceea, în sistemul cu baza 12 am avea mai multe numere „rotunde“, ceea ce ar permite stabilirea mai multor procedee prescurtate pentru efectuarea operațiilor. În ansamblu, însă, avantajul nu ar fi prea mare.

În sistemul de numerație cu baza 12 am fi nevoiți să introducem, pe lîngă zero și cifrele de la 1 la 9, încă două cifre pentru notarea lui 10 și a lui 11. Vom conveni să notăm aceste cifre cu simbolurile **X** și **A**. Să scriem, de exemplu, numărul 1443 în sistemul cu baza 12:

$$\begin{array}{r} 1443 \\ -12 \\ \hline 24 \\ -24 \\ \hline 3 \end{array} \quad \begin{array}{r} 12 \\ -120 \\ \hline 120 \\ -120 \\ \hline 0 \end{array} \quad \begin{array}{r} 12 \\ 10 \end{array}$$

¹⁾ Spre deosebire de notațiile adoptate în algebră, expresia $abcdk$ de aici nu înseamnă produsul numerelor a, b, c, d și k , ci numărul scris într-un sistem de numerație pozițional arbitrar cu ajutorul cifrelor a, b, c, d, k .

Ultimul cit este egal cu zece, iar resturile sînt zero și trei. Prin urmare, $1443 = X03$.

În toate problemele studiate pînă aici am indicat sistemele de numerație și am cerut să fie exprimate în aceste sisteme anumite numere date. Se pot pune și alte probleme. De exemplu, după notația dată a unor operații cu numere să se stabilească ce sistem de numerație s-a folosit. Iată un exemplu pentru o astfel de problemă. Se dă notația

$$\begin{array}{r} 121 \\ \times \\ 22 \\ \hline 242 \\ + \\ 242 \\ \hline 3212. \end{array}$$

În ce sistem de numerație sînt corecte aceste operații?

Examinînd cu atenție efectuarea operațiilor, observăm că $2+4$ dau un număr care se termină cu 1¹⁾. Însă „doi“ și „patru“ fac „șase“, indiferent de felul în care le-am scrie. Deci, sistemul de numerație dat nu cuprinde un simbol pentru numărul „șase“. Am găsit însă cifra 4 (patru) în notația noastră. Prin urmare, sistemul de numerație poate avea ori baza 5, ori baza 6. Scriind numărul „șase“ în aceste două sisteme, obținem 11 (baza 5) și 10 (baza 6). Prin urmare, în exemplul nostru, în care $2+4$ dau un număr care se termină cu o unitate, sistemul de numerație are baza 5. Iată încă un exemplu ușor; în ce sistem de numerație avem $3 \times 3 = 10$? Cititorul va vedea imediat că aceasta este posibil numai pentru baza nouă.

Nu totdeauna însă se poate stabili precis, după aspectul unei operații, în ce sistem de numerație este valabilă notația. De exemplu, egalitatea $122 \times 3 = 366$ este valabilă în orice sistem de numerație cu baza mai mare decît 6.

Se întîmplă însă ca și „biete resturi“ ale unei operații să ne poată ajuta la stabilirea sistemului de numerație în care este scrisă această operație și chiar la reconstituirea ei. Iată un

¹⁾ Se presupune că cifrele reprezintă aceleași numere ca și în sistemul nostru de numerație, cu alte cuvinte că 1 este simbolul unității, 2 al numărului „doi“ etc.

exemplu : să presupunem că sînt cunoscute numai unele cifre din următoarea operație (celelalte sînt înlocuite cu steluțe):

$$\begin{array}{r} \text{**2} \\ \times \\ \text{*2} \\ \hline \text{*00*} \\ + \\ \text{***1} \\ \hline \text{****1.} \end{array}$$

În ce sistem de numerație este scrisă această operație? Cum să reconstituim cifrele lipsă?

Să privim mai întîi ultimele cifre ale deînmulțitului și ale înmulțitorului, percum și ultima cifră a rezultatului. Vedem că numărul „patru” (de două ori doi) se termină cu o unitate în acest sistem de numerație, adică nu avem pentru el un semn special. Aceasta este posibil numai dacă baza nu depășește patru, adică dacă baza este 2, 3 sau 4. În baza 2 numărul patru (pătratul bazei) se scrie 100; în baza 3, numărul patru se scrie 11 (adică $3 \cdot 1 + 1$). În sfîrșit, în baza 4, numărul patru (baza în-săși) se scrie 10. Așadar, baza căutată nu poate fi decît numărul trei.

Notînd, mai departe, a doua cifră a deînmulțitului cu x și ținînd în minte o unitate, $2x+1$ ne dă un număr care se termină cu zero; aceasta este posibil numai pentru $x=1$ ¹⁾. Tot astfel, găsim că prima cifră a deînmulțitului este egală cu unitatea. Prin urmare, deînmulțitul este 112, adică numărul patrusprezece.

Cifra din stînga a înmulțitorului, înmulțită cu doi, ne dă un număr care se termină cu 1. Însă $2 \cdot 0 = 0$, $2 \cdot 1 = 2$, $2 \cdot 2 = 11$. Prin urmare, această cifră poate fi egală numai cu 2, înmulțitorul este 22 (opt) și toată operația se scrie astfel:

$$\begin{array}{r} 112 \quad \text{sau în sistemul nostru} \quad 14 \\ \times \quad \text{de numerație:} \quad \times \\ 22 \quad \quad \quad 8 \\ \hline 1001 \quad \quad \quad 112 \\ + \\ 1001 \\ \hline 11011 \end{array}$$

¹⁾ x poate fi egal cu 0, cu 1 sau cu 2 (dat fiind că sistemul de numerație are baza trei). Însă $2 \cdot 0 + 1 = 1$; $2 \cdot 1 + 1 = 10$; $2 \cdot 2 + 1 = 12$. Așadar x trebuie să fie egal cu 1.

Pentru verificare, să scriem 112 în sistemul de numerație cu baza 3:

$$\begin{array}{r} 112 \mid 3 \\ - 9 \mid 37 \\ \hline 22 \mid 3 \\ - 21 \mid 7 \\ \hline 1 \mid 6 \\ \hline 1 \end{array} \quad \begin{array}{r} 3 \\ - 12 \\ \hline 12 \\ - 12 \\ \hline 0 \end{array} \quad \begin{array}{r} 3 \\ - 4 \\ \hline 3 \\ - 3 \\ \hline 1 \end{array} \quad \begin{array}{r} 3 \\ - 1. \\ \hline 1. \end{array}$$

Obținem tocmai 11011.

Să trecem de la exemple la concluzii generale. Cu cît este mai mică baza sistemului de numerație, cu atît devine mai greoaie scrierea numerelor și a operațiilor cu ele. Iată, de exemplu, cum arată înmulțirea lui douăzeci și trei cu șaptesprezece în sistemul zecimal și în sistemul ternar:

în sistemul zecimal :	$\begin{array}{r} 23 \\ \times \\ 17 \\ \hline 161 \\ + \\ 23 \\ \hline 391 \end{array}$	în sistemul ternar :	$\begin{array}{r} 212 \\ \times \\ 122 \\ \hline 1201 \\ + 1201 \\ \hline 212 \\ \hline 112111 \end{array}$
--------------------------	--	-------------------------	---

Scrierea în sistemul ternar ocupă mai mult loc decît în cel zecimal și este deci mai greoaie. În ceea ce privește calculul însuși, în scris, ne dăm ușor seama că el este considerabil mai simplu în sistemul ternar decît în cel zecimal.

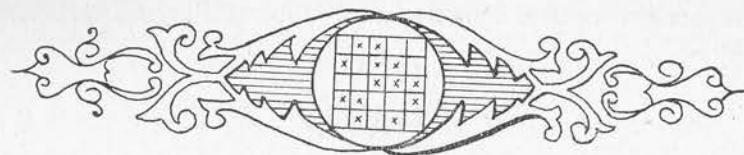
În adevăr, pentru a calcula „pe coloană” în mod obișnuit trebuie să ținem minte „tabla adunării” și „tabla înmulțirii”. „Tabla adunării” ne-o însușim treptat, în curs de doi-trei ani; cît privește învățarea tablei înmulțirii, ea este legată, probabil pentru fiecare, de amintiri nu tocmai plăcute.

Cînd baza este mică, tabla adunării și tabla înmulțirii sînt considerabil mai simple decît în sistemul zecimal. Iată aceste table pentru baza trei:

$0+0=0$;	$1+0=1$;	$2+0=2$
$0+1=1$;	$1+1=2$;	$2+1=10$
$0+2=2$;	$1+2=10$;	$2+2=11$
$0 \times 0 = 0$;	$1 \times 0 = 0$;	$2 \times 0 = 0$
$0 \times 1 = 0$;	$1 \times 1 = 1$;	$2 \times 1 = 2$
$0 \times 2 = 0$;	$1 \times 2 = 2$;	$2 \times 2 = 11$

Este limpede că aceste table se învață mult mai ușor decât cele corespunzătoare pentru sistemul zecimal.

Cel mai mic număr natural care poate servi ca bază într-un sistem de numerație este doi. În acest sistem, operațiile trebuie să se efectueze deosebit de ușor. În capitolul următor ne vom convinge că așa și este în realitate. La numerația pozițională cu baza doi aproape toate calculele se efectuează automat: obținem un fel de „aritmetică în care nu trebuie să socotim“.



CAPITOLUL V

O ARITMETICĂ ÎN CARE NU TREBUIE SĂ SOCOTIM



Sistemul de numerație avînd ca bază numărul doi are multe proprietăți remarcabile. Merită să insistăm asupra lui. În acest sistem se folosesc numai două simboluri pentru scrierea numerelor: semnul pentru unitate (1) și intervalul pozițional, zero (0).

În acest capitol, ca și în cel precedent, numerele scrise în sistemul binar vor fi imprimate cu caractere grase, iar cele scrise în sistemul zecimal, cu caractere obișnuite.

Pentru unitate, avem semnul **1**. Numărul doi, care este baza sistemului de numerație, va deveni o unitate de ordinul al doilea și se va scrie **10**. Numărul trei, format dintr-o unitate de ordinul al doilea (doi) și dintr-o unitate de ordinul întâi, se scrie **11**. Patru este pătratul lui doi, adică o unitate de ordinul al treilea, deci se va scrie **100**. În ceea ce privește numărul opt, egal cu doi la cub, el va trebui scris ca mia noastră obișnuită: **1000**.

Observăm că numerele care au în sistemul zecimal o singură cifră, în aritmetica binară sînt de cîte trei și chiar de patru cifre. Mai departe vom vedea că scrierea operațiilor ocupă de asemenea mult mai mult loc decât în sistemul zecimal. Toate acestea fac ca sistemul binar să fie, practic, puțin utilizabil. Însă simplitatea efectuării operațiilor în acest sistem este cu adevărat uluitoare.

Să începem cu adunarea. De exemplu să adunăm **10110** și **1101** (adică 22 și 13).

Să scriem aceste numere unul sub altul, cum procedăm obișnuit,

$$\begin{array}{r} 10110 \\ + \\ 1101 \\ \hline \end{array}$$

Dacă într-o coloană avem o singură unitate (cifra a doua fiind zero), atunci o scriem dedesubtul liniei. Dacă avem însă două unități, ca în coloana a treia, atunci le tăiem, scriem jos zero și sus, deasupra ordinului următor, adăugăm o unitate. Procedăm la fel cu ordinul următor, ținând seama și de unitățile scrise deasupra. Intreaga operație arată astfel:

$$\begin{array}{r} 111 \\ + 10110 \\ + 1101 \\ \hline 100011 \end{array}$$

În fond, facem același lucru ca și în notațiile obișnuite, numai că nu trebuie să calculăm de loc: nu punem decât bare și zerouri și tăiem bare. Iată un exemplu mai complicat (în dreapta el este scris în sistemul zecimal),

$\begin{array}{r} 111111 \\ 1111111 \\ \hline 101101 \\ + 11011 \\ + 10001 \\ \hline 101011 \\ \hline 10000100 \end{array}$	$\begin{array}{r} 12 \\ \hline 45 \\ 27 \\ + \\ 17 \\ 43 \\ \hline 132 \end{array}$
---	---

După ce am tăiat două unități în coloana din extrema dreaptă, punem deasupra celei de-a doua coloane (deasupra liniei) o unitate în plus; tăind încă două unități, mai punem o unitate în plus. Coloana din dreapta nu mai cuprinde alte unități. De aceea scriem zero sub linia de jos. Același lucru se va întâmpla și cu a doua coloană din dreapta; aici va trebui să ținem seama și de unitățile de deasupra liniei de sus. În coloana a treia (din dreapta) există trei unități. Tăiem două dintre ele scriind o unitate deasupra coloanei a patra, iar pe a treia o scriem sub linia de jos etc.

Notația este foarte greoaie în comparație cu scrierea noastră zecimală. În schimb, operația se efectuează automat.

Scăderea se efectuează foarte simplu dacă folosim „regula complementului”. Se numește complement zecimal al unui număr dat diferența dintre cea mai apropiată putere a lui zece („unu cu zerouri”) mai mare decât acest număr și numărul considerat. De exemplu, complementul zecimal al numărului 7 este 3, al numărului 89 este 11, al numărului 6385 este 3615, iar al numărului 580 este 420. Pentru a găsi complementul, trebuie să scădem toate cifrele numărului dat din nouă, iar pe ultima (fără a ține seama de zerourile de la sfârșit) din zece. Acum nu mai este greu să înlocuim scăderea prin adunare: în loc să scădem un număr din altul dat, este suficient să adăugăm la acesta din urmă complementul zecimal al scăzătorului și să scădem puterea lui zece. De exemplu, scăzând 5833 din 11021, așezăm operația astfel:

$$\begin{array}{r} 11021 \\ + \\ 4167 \\ \hline 15188 - 10000 = 5188 \end{array}$$

Analog cu complementul zecimal se introduce și complementul binar. Se numește complement binar al unui număr dat diferența dintre puterea lui doi, cea mai apropiată de acest număr, și numărul dat. Complementul binar al unui număr scris în sistemul de numerație binar se află mai simplu decât complementul zecimal. De exemplu, să presupunem că trebuie găsit complementul binar al numărului 11010111000. Ultima unitate din dreapta și toate zerourile care-i urmează (dacă avem zerouri) rămân neschimbate, iar în tot restul înlocuim unitățile cu zerouri și zerourile cu unități. Dacă vom obține în rezultat zerouri în stînga, acestea se suprimă pînă la prima unitate. Astfel, din numărul 11010111000, obținem numărul

$$00101001000$$

adică 101001000. Acesta este complementul binar al numărului 11010111000.

Din moment ce știm să aflăm complementul binar, putem efectua automat scăderea. De exemplu, să efectuăm

$$1110001 - 11011 = ?$$

Aflăm mai întîi complementul binar al scăzătorului:

$$00101 = 101$$

Inlocuim apoi scăderea printr-o adunare :

$$\begin{array}{r} 1 \\ 1110001 \\ + \quad 101 \\ \hline 1110110 - 100000 = 1010110 \end{array}$$

În sistemul zecimal, scăderea acelorași numere se va scrie mai simplu : $113 - 27 = 86$.

Scrierea greoaie din sistemul binar face ca automatismul efectuării operațiilor de adunare și scădere să-și piardă orice valoare. În schimb, la înmulțire caracterul automat este evident și scrierea greoaie nu anulează deosebita simplitate a operației.

Tabla înmulțirii în sistemul de numerație binar are următoarea formă :

$$0 \times 0 = 0; \quad 0 \times 1 = 0; \quad 1 \times 0 = 0; \quad 1 \times 1 = 1.$$

Operația se scrie în aceeași ordine ca și în notațiile obișnuite. De exemplu, să înmulțim numărul 111001101 cu 1101101 :

$$\begin{array}{r} 111001101 \\ \times \quad 1101101 \\ \hline 11 \\ 111111111 \\ 111111111111 \\ \hline 111001101 \\ 111001101 \\ + \quad 111001101 \\ \hline 111001101 \\ 111001101 \\ \hline 1100010001001001 \end{array}$$

ceea ce corespunde în sistemul zecimal la :

$$\begin{array}{r} 461 \\ \times \quad 109 \\ \hline 4149 \\ + \quad 461 \\ \hline 50249 \end{array}$$

(La înmulțirea binară tragem sub înmulțitor două linii pentru a lăsa între ele loc unităților care se vor obține în urma adunării și pe care, la înmulțirea obișnuită, le ținem minte.)

Scrierea zecimală este considerabil mai compactă, așa cum se observă și din exemplul dat. Însă efectuarea unei înmulțiri zecimale între numere cu mai multe cifre presupune o anumită calificare. Este nevoie de ani de muncă pentru a-l învăța pe copil să efectueze fără greșală o astfel de înmulțire. Dimpotrivă, înmulțirea binară se realizează complet automat.

Cea mai dificilă dintre operațiile aritmetice este, incontestabil, împărțirea. Cu siguranță că oricine ține minte cât de complicată i se părea împărțirea în copilărie. De altfel, nici un om matur nu va fi prea încântat, dacă va trebui să împartă, de exemplu 8 663 545 198 prin 87 995. În evul mediu împărțirea era considerată drept o operație atât de dificilă, încât oamenilor îndemnatici în efectuarea ei li se confereau titluri academice.

În sistemul de numerație binar, împărțirea se efectuează însă perfect automat! Ce este drept, simplitatea și automatismul sînt răscumpărate aici printr-o scriere neobișnuit de greoaie. Ca exemplu, vom împărți 11011101 prin 10111. Operația se scrie în același fel ca și la împărțirea obișnuită, însă de fiecare dată vom scrie sub deîmpărțit, nu produsul împărțitorului cu cifra corespunzătoare a cîtului, ci complementul binar al acestui produs (putem eventual să nu ștergem zerourile):

$$\begin{array}{r} 1 \quad 11 \\ 11011101 \quad | \quad 10111 \\ + \quad 01001 \quad | \quad 1001 \\ \hline 100100 \\ - \quad 100000 \quad 1 \\ \hline 100101 \\ + \quad 01001 \\ \hline 101110 \\ - \quad 100000 \\ \hline 1110 \end{array}$$

$$\begin{array}{r} 221 \quad | \quad 23 \\ - 207 \quad | \quad 9 \\ \hline 14 \end{array}$$

Obținem cîtul 1001 și restul 1110. În dreapta dăm aceeași împărțire în scrierea zecimală. Se vede imediat că sistemul binar este practic inaplicabil, deoarece scrierea sa este foarte greoaie¹⁾. În schimb însă nu trebuie să calculăm, să facem încercări sau să observăm ceva.

Primul european care a atras atenția asupra deosebitei simplități a sistemului de numerație binar și asupra specificului său a fost celebrul filozof și matematician G. W. Leibniz (1646—1716). Se pare însă că matematicienii chinezi și-au dat seama de aceasta cu mult înainte.

¹⁾ În ultimul timp sistemul binar și-a găsit aplicații importante la mașinile electronice de calcul. (N. Red. E. T.)

Sistemul de numerație binar are aplicații variate în diverse capitole ale matematicii și în tehnică. Este foarte greu să vorbim despre ele în această carte, destinată unui cititor fără pregătire de specialitate. În schimb, vom da câteva probleme în care ies în evidență particularitățile acestui sistem.

Majoritatea aplicațiilor sistemului binar se bazează pe următoarea proprietate specifică a acestuia. În sistemul binar, o unitate de orice ordin poate sau să figureze (și atunci neapărat este singura) sau să lipsească, pe cînd în toate celelalte sisteme de numerație trebuie să indicăm câte unități de fiecare ordin fac parte dintr-un număr dat (de exemplu enunțînd sau scriind numărul nouă sute cincizeci și unu observăm că el conține nouă sute, cinci zeci și o unitate). Cînd scriem un număr în sistemul binar nu este necesar să specificăm câte unități de ordinul al treilea, câte de al doilea și câte de primul ordin are. Este suficient să spunem că există, de exemplu, unitate de ordinul al treilea, nu există unitate de ordinul al doilea, există unitate de ordinul întîi. În modul acesta am determinat perfect care este numărul: **101**, corespunzător lui 5 din sistemul zecimal. De exemplu, cu ce este egal un număr în care avem o unitate de ordinul al zecelea, nu avem unități de ordinele al nouălea, al optulea și al șaptelea, avem unități de al șaselea și de al cincilea ordin și nu avem unități de la al patrulea în jos? Imediat găsim acest număr: **1000110000**, adică 560 din sistemul zecimal.

Toate acestea se pot exprima și altfel. Să considerăm un șir de numere care încep cu unitatea, fiecare număr fiind de două ori mai mare decît precedentul (progresie geometrică):

$\div 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, \dots$
 $\uparrow$ 1 2 3 4 5 6 7 8 9 10...

Orice număr poate fi reprezentat ca o sumă de mai mulți termeni ai acestui șir. De exemplu, 19 este egal cu suma primului, al doilea și al cincilea termen (rangul fiecărui termen este notat cu cifre mici dedesubt); numărul 100 este egal cu suma termenilor al treilea, al șaselea și al șaptelea etc. În adevăr, orice număr poate fi scris în sistemul de numerație binar: unitățile ne vor indica termenii din această progresie care figurează în numărul respectiv, iar zerourile ne vor indica termenii care lipsesc ($19 = 10011$, $100 = 1100100$).

Acum nu este greu să explicăm următorul joc distractiv. Propuneți partenerului să se gîndească la un număr cuprins între 1

și 31, apoi îi dați cartonul cu tabela din fig. 3 și cereți-i ca, fără să vă arate tabela, să spună în ce linii se află numărul; de îndată ce el vă va spune numerele liniilor, veți putea să ghiciți numărul la care s-a gîndit.

Nº1	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31
Nº2	2	3	6	7	10	11	14	15	18	19	22	23	26	27	30	31
Nº3	4	5	6	7	12	13	14	15	20	21	22	23	28	29	30	31
Nº4	8	9	10	11	12	13	14	15	24	25	26	27	28	29	30	31
Nº5	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31

Fig. 3

Această tabelă este întocmită foarte simplu. În prima linie figurează toate numerele de la 1 pînă la 31, care au în scrierea binară o unitate drept primă cifră din dreapta (adică toate numerele impare). În linia a doua figurează toate numerele care au o unitate în locul al doilea din dreapta. De exemplu, numărul trei, care se scrie în sistemul binar **11**, figurează atît în linia întîi, cît și în a doua, deoarece primele sale două cifre din dreapta sînt unități. În același mod sînt alcătuite și celelalte linii. În ultima linie figurează toate numerele cuprinse între 1 și 31, care au în scrierea binară cifra a cincea din dreapta **1**, adică numerele de la 16 pînă la 31.

Să presupunem că partenerul s-a gîndit la numărul 29. El vede că acest număr figurează în prima linie, în a treia, în a patra și în a cincea. Spunîndu-vă aceste linii, el vă indică, fără să-și dea seama, că în scrierea binară numărul la care s-a gîndit are cîte o unitate de ordinele întîi, al treilea, al patrulea și al cincilea. Știți că în sistemul binar unitățile de aceste ordine sînt numerele 1, 4, 8 și 16 (ele figurează în prima coloană a tabelii). Acum este ușor să reconstituiți aproape instantaneu numărul la care s-a gîndit partenerul: trebuie numai să adunați în minte cele cîteva numere mici, iar rezultatul va fi 29.

Se mai poate imagina și un alt joc distractiv de efect. Trebuie doar să învățăm a memora repede cîteva numere de cîte două cifre (ca și cum am reține două numere de telefon, ceea ce nu este greu, cu atît mai mult cu cît ele trebuie memorate doar cîteva minute). Jocul consistă în următoarele: propuneți parte-

nerului să deseneze un pătrat din 5×5 celule și să dispună în mod arbitrar cruciulițe în aceste celule. Apoi, timp de o jumătate de minut, examinați cu atenția pătratul și-l restituiți partenerului. Vă obligați apoi ca peste cinci minute să redesenați din memorie dispoziția cruciulițelor, ceea ce veți reuși imediat. Cei din jur își vor închipui că este ceva foarte simplu, însă cereți oricăruia dintre ei să memoreze într-o jumătate de minut dispoziția cruciulițelor din pătrat: puteți fi sigur că nimeni nu va reuși!

Care este secretul memorizării rapide a dispoziției cruciulițelor în tabela pătrată? Cel mai simplu este să recurgem la un exemplu. Fie dată următoarea dispoziție a cruciulițelor:

	x	x		
x		x	x	
		x	x	x
x	x			x
	x		x	

Considerați cruciulițele drept unități, iar celulele goale, zerouri. Atunci fiecare linie poate fi considerată ca un număr scris în sistemul binar. În exemplul nostru avem următoarele numere:

1100,
10110,
111,
11001,
1010

(zerourile din stînga unităților au fost omise). Aceste numere se citesc ușor:

1100 = 12,
10110 = 22,
111 = 07,
11001 = 25,
1010 = 10.

Cu un oarecare antrenament această convertire din sistemul binar în cel zecimal se realizează aproape instantaneu. Ne rămîne să memorăm șirul de numere: 12, 22, 07, 25, 10. Pentru convertirea din sistemul binar în cel zecimal și pentru memorarea acestui șir, o jumătate de minut este suficientă, dacă am exersat suficient înainte.

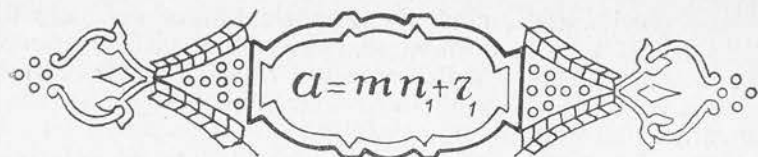
După cinci minute, cînd din memoria tuturor s-a șters dispoziția cruciulițelor, continuați să țineți minte șirul de numere. După aceste numere puteți reconstitui imediat tabela inițială: este suficient să le scrieți unul sub altul în sistemul de numerație binar, înlocuind unitățile cu cruciulițe.

Această posibilitate de a folosi sistemul de numerație binar ca procedeu pentru memorarea tabelor pătratice se folosește la cifrare și la criptografie. Modul cum se realizează aceasta este relatat amănunțit în cartea lui Я. И. Перельман, «Живая математика», Гостехиздат, М.—Л., 1946.

Cititorul va observa că în toate raționamentele noastre există ceva neriguros. Am folosit de cîteva ori expresia: „orice număr (întreg) poate fi scris într-un sistem de numerație pozițional cu orice bază”. Oare așa să fie? Raționamentele pe care le-am folosit în capitolul precedent, scriind același număr în sisteme cu baze diferite, arată că aceasta este probabil adevărat. Problema va fi tratată mai profund în cele ce urmează, la sfîrșitul capitolului VI (p. 60); acolo vom demonstra riguros posibilitatea de a reprezenta orice număr într-un sistem pozițional cu orice bază.

În încheiere, vom face cîteva observații. Așa cum în sistemul de numerație zecimal putem scrie numere întregi și fracționare (fracții zecimale), tot astfel putem introduce fracții binare, ternare etc. Aceste fracții au aplicații interesante, însă cartea noastră este consacrată numai numerelor întregi și de aceea nu ne vom putea ocupa de ele.





CAPITOLUL VI

MĂSURA COMUNĂ



Adunarea și înmulțirea — cele două operații directe — se bucură de următoarea proprietate importantă: ele sînt întotdeauna posibile în numere întregi. Mai exact, dacă sînt date două numere naturale arbitrare, putem găsi întotdeauna un număr natural egal cu suma lor și un număr natural egal cu produsul lor. Situația se prezintă altfel în cazul operațiilor inverse: al scăderii și împărțirii. Nu întotdeauna putem găsi un număr natural egal cu diferența a două numere naturale date (de exemplu nu există un număr natural egal cu $5-8$ sau $6-6$); tot astfel, nu reușim totdeauna să găsim un număr natural egal cu cîțul a două numere naturale (de exemplu nu există un număr natural egal cu $5:8$). Între scădere și împărțire există însă o deosebire esențială. Astfel, putem afla foarte simplu dacă un număr natural se poate scădea sau nu din altul. Există un „criteriu al scăderii”, unic și universal: dacă numărul b este mai mare decît numărul a , sau egal cu el, nu putem să-l scădem pe b din a , adică nu putem găsi un număr natural egal cu $a-b$. Dimpotrivă, la împărțire adeseori este greu să aflăm dacă numărul a se împarte sau nu prin b (adică dacă a/b este sau nu un număr natural).

Mai mult, din orice număr natural (cu excepția lui 1) putem scădea toate numerele mai mici decît acesta. Diversii scăzători posibili ai numărului N vor fi întotdeauna în număr de $N-1$ (de exemplu, pentru numărul 5, scăzătorii posibili vor fi numerele 1, 2, 3, 4, adică în total $N-1=5-1=4$ numere). În cazul împărțirii, însă, situația este mult mai complicată. Există un număr care are un singur divizor: acesta este 1. Există numere care au

doi divizori: 1 și numărul însuși (astfel sînt numerele 2, 3, 5, 7 etc.). În sfîrșit, există numere care au mai mult decît doi divizori; așa de exemplu, numărul 6 are patru divizori (1, 2, 3 și 6). Numerele care au numai doi divizori se bucură de multe proprietăți remarcabile. Ele se numesc numere prime.

Așadar, chiar cea mai superficială privire de ansamblu asupra operațiilor aritmetice cu numere naturale pune două probleme, aparent foarte simple. Prima dintre ele consistă în a găsi criteriile („regulile de divizibilitate”) care ne permit să aflăm dacă un număr se împarte sau nu prin altul (astfel ca să obținem un număr natural la cît). A doua problemă consistă în a studia proprietățile numerelor prime. Ambele, și îndeosebi a doua, prezintă dificultăți mult mai mari decît pare la prima vedere. În studiul lor matematicienii s-au lovit de multe chestiuni noi. Unele dintre aceste chestiuni au rămas nerezolvate pînă în zilele noastre, deși matematicienii studiază numerele prime de peste 2000 de ani. Regulile de divizibilitate și teoria numerelor prime formează obiectul principal al teoriei divizibilității — un capitol foarte important al teoriei numerelor, despre care a fost vorba în introducerea cărții noastre.

Pentru a ne familiariza cu unele probleme ale teoriei numerelor, trebuie să ne reamintim și să aprofundăm cîteva definiții și teoreme fundamentale din cursul școlar de aritmetică.

Să începem cu următoarele. Dacă există un număr natural n egal cu cîțul împărțirii numărului a prin b , adică un număr care înmulțit cu b să de a , atunci spunem că a este multiplul lui b , sau că a este divizibil sau se împarte prin b . Numărul b se numește divizor al numărului a . Astfel, 6 este un multiplu al lui 2; 15 este divizibil prin 5 etc. Faptul că b este un divizor al lui a se exprimă prin următoarea formulă:

$$a = bn,$$

unde n este un număr natural.

În teoria divizibilității trebuie să recurgem permanent la trei teoreme din aritmetică, pe care le vom întîlni cînd în majoritatea raționamentelor ce vor urma. Deși este poate plictisitor, ne vom opri aici asupra lor, pentru ca în capitolele următoare să nu ne mai abată atenția de la esența problemelor.

Teorema 1. *Dacă a este divizibil prin b , iar b , la rîndul său, este divizibil prin c , atunci a este divizibil prin c .*

Teorema 2. *Dacă suma algebrică (adică suma sau diferența aritmetică) a mai multor numere este egală cu zero sau este divizibilă printr-un număr N și toți termenii, în afară de unul*

despre care nu știm nimic, sînt multipli ai lui N , atunci și acest din urmă termen va fi divizibil prin N .

Teorema 3. Dacă produsul a două numere întregi a și b se împarte printr-un număr m , care nu are divizori comuni cu a (bineînțele, în afară de unitate), atunci b este divizibil prin m .

Primele două teoreme sînt absolut clare. Dacă 36 este divizibil prin 9, iar 9, la rîndul său, se împarte cu 3, înseamnă că și 36 trebuie să se împartă prin 3. Tot astfel, dacă $3-x-9+81=0$, este clar că x trebuie să fie un multiplu de 3. Aceste teoreme trebuie demonstrate, nu pentru a convinge pe cineva de adevărul lor, ci pentru a arăta cum sînt legate de alte propoziții mai simple. Cititorul le va demonstra fără dificultate. În ceea ce privește a treia teoremă, ea se demonstrează mai greu, cu toată simplitatea ei aparentă. Vom reveni asupra acestei teoreme la p. 54.

Înainte de a trece mai departe, să ne ocupăm de împărțirea cu rest. Dacă înmulțirea cu un număr întreg poate fi considerată ca o adunare repetată, este firesc să considerăm împărțirea drept o scădere repetată. De exemplu, pentru a împărți 20 prin 5, vom scădea 5 din 20; după prima scădere, vom obține 15, după a doua 10, după a treia 5, după a patra zero (în studiul problemelor de divizibilitate, este comod să adăugăm numărul zero la numerele naturale, considerînd, astfel, toate numerele întregi care nu sînt negative). Așadar, în acest caz sînt posibile patru scăderi consecutive; aceasta înseamnă că împărțirea lui 20 prin 5 dă cîtu 4. Persoanele care au avut ocazia să lucreze cu sciutul sau cu aritmometrul, vor socoti aceste considerații asupra împărțirii cît se poate de firești. Nu este greu de observat că numărul de scăderi consecutive este egal cu acel număr care, înmulțit cu împărțitorul (cu scăzătorul repetat) va da deîmpărțitul (numărul inițial).

Deoarece în capitolul de față și în cele imediat următoare vom considera alături de numerele naturale și numărul zero, enunțăm aici proprietățile lui. În primul rînd, trebuie arătat că nici un număr nu poate fi împărțit prin zero. În adevăr, cu ce poate fi egal $a:0$, pentru $a \neq 0$? Cu nici un număr, dat fiind că orice număr înmulțit cu zero va da zero și nu a . Dacă vom încerca însă să împărțim pe zero prin zero, vom putea lua drept cît orice număr, dat fiind că orice număr înmulțit cu zero dă zero. Din această cauză, este strict interzis în matematică să împărțim prin zero. Dimpotrivă, numărul zero poate fi împărțit prin orice număr (diferite de zero), cîtu fiind totdeauna zero. Cînd vorbim despre împărțirea numerelor întregi, însă nu neapărat naturale, ajungem la concluzia că zero se împarte fără rest prin orice număr întreg

care nu este nul, deoarece $0:a=0$, iar zero se consideră număr întreg. Bazîndu-ne pe aceasta, obișnuim să spunem că zero este multiplul oricărui număr.

Scăderea repetată este aplicabilă și atunci cînd deîmpărțitul nu este multiplu al împărțitorului. În acest caz, ultima scădere nu ne va da zero, ci un număr mai mic decît împărțitorul, care se numește r e s t. De exemplu, să împărțim 17 prin 5, folosind metoda scăderii succesive. Scăzînd pe 5 din 17 prima dată obținem 12; la a doua scădere obținem 7, la a treia 2. Mai departe nu putem scădea. Așadar, cîtu împărțirii lui 17 prin 5 va fi egal cu numărul de scăderi consecutive, adică 3, iar restul va fi numărul 2.

Scăderea consecutivă a numărului b din numărul a , în care obținem cîtu n și restul r , se poate scrie compact astfel:

$$\underbrace{a-b-b-\dots-b}_{\text{de } n \text{ ori}} = r \quad (0 < r < b)$$

reducerea termenilor asemenea dă $a-bn=r$ sau $a-r=bn$, ceea ce revine la a spune: dacă din numărul a scădem restul r rezultat din împărțirea lui a prin b , diferența $a-r$ va fi divizibilă prin b .

Mai importantă este următoarea așezare a termenilor în formulă:

$$a=bn+r \quad (0 < r < b).$$

Aceasta este formula fundamentală de definiție a împărțirii cu rest. Trebuie subliniat faptul că r este totdeauna mai mic decît b . Dacă r este nul, împărțirea se efectuează exact. Pentru a nu elimina acest caz, vom introduce în formulă și semnul de egalitate ($r=0$), legîndu-l de semnul inegalității. Vom avea astfel:

$$a=bn+r \quad (0 \leq r < b).$$

Din raționamente reiese clar că numerele n și r sînt determinate în mod unic prin numerele a și b . Cu alte cuvinte, dacă sînt date două numere a și b ($a > b$), atunci cîtu n și restul r sînt unic determinate; restul este nenegativ (adică pozitiv sau nul) și întotdeauna mai mic decît împărțitorul.

Să părăsim pentru puțin timp manualele de aritmetică moderne și să vedem cum era abordată problema divizibilității în urmă cu peste 2000 de ani de către Euclid, unul dintre cei mai mari matematicieni greci. În opera sa „Elemente”, compusă din 13 „cărți”, el a sintetizat și sistematizat cunoștințele de matematică ale timpului. „Elementele” lui Euclid sînt atît de bine elaborate, încît pînă acum vreo 100 de ani în școlile din Anglia, geometria se studia direct după cartea lui Euclid, folosită ca

manual. În fond, „Elementele” sînt consacrate geometriei, însă ele se ocupă și de unele probleme de aritmetică; astfel cartea a cincea este consacrată teoriei proporțiilor, a zecea, clasificării mărimilor iraționale, iar cărțile a șaptea, a opta și a noua se ocupă de aritmetica numerelor întregi. Între altele „Elementele” studiază aflarea măsurii comune a două segmente și problema înrudită a aflării celui mai mare divizor comun a două numere întregi. Procedeu pe care îl folosim pentru a obține cel mai mare divizor comun a două numere și-a păstrat de altfel numele de *algoritm* lui Euclid¹⁾.

Se numește *măsură comună* a două segmente un al treilea segment care poate fi purtat de un număr întreg de ori pe fiecare dintre cele două segmente date. De exemplu, să găsim măsura comună a segmentelor AB și CD din fig. 4. Așezăm segmentul mai mic CD peste cel mare AB , pornind din punctul A , de cîte ori va fi posibil. Dacă CD se cuprinde în AB de un număr întreg de ori, fără rest, el va fi, evident, măsura comună. Dacă însă, cum este cazul în desenul nostru, va rămîne un rest D_3B , va trebui să căutăm măsura comună a celui mai mic dintre segmente CD și a restului D_3B , adică să luăm pe CD , începînd din punctul C , unul după altul segmente egale cu D_3B . În fig. 4, segmentul CD poate fi purtat exact de patru ori pe CD . Segmentul CD se cuprinde în AB de trei ori, cu un rest egal cu D_3B . Așadar, D_3B se cuprinde în AB exact de $4 \cdot 3 + 1 = 13$ ori. Prin urmare, D_3B se cuprinde de un număr întreg de ori și în AB (de 13 ori) și în CD (de 4 ori). El este măsura comună a acestor segmente.

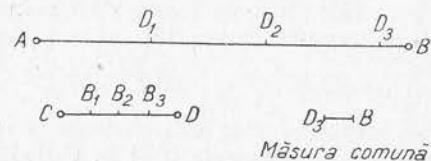


Fig. 4

Nu întotdeauna aflarea măsurii comune se desfășoară atît de repede și simplu. Se poate întîmpla ca restul să nu se cuprindă de un număr întreg de ori în segmentul mai mic. În acest caz vom obține un segment nou (al doilea rest), care va trebui purtat în lungul primului segment-rest. Dacă unul dintre resturile succesive (al cincilea, al zecelea, al o sutălea, al miilea,...) se va

¹⁾ Se numește *algoritm* o regulă care ne permite să rezolvăm în mod automat o anumită problemă de matematică, să efectuăm un anumit calcul etc.

cuprinde de un număr întreg de ori în cel precedent, el va fi măsura comună a celor două segmente inițiale.

Se întîlnesc însă și situații mai dificile. Se poate întîmpla ca această purtare succesivă a fiecărui nou rest pe cel precedent să nu se termine niciodată. De fiecare dată vom obține cîte un alt rest. În acest caz nu putem găsi o măsură comună a celor două segmente, deoarece ea nu există. Astfel este cunoscut că latura pătratului și diagonala lui nu au o măsură comună.

Și în aritmetica numerelor întregi putem pune problema măsurii comune a două numere, adică a unui număr care să se cuprindă de un număr întreg de ori în fiecare dintre ele, adică cele două numere date să se împartă prin el fără rest. Spre deosebire de segmente, la numerele întregi există întotdeauna această măsură comună: numărul unu, care „se cuprinde” de un număr întreg de ori în orice număr întreg. Însă, pe lîngă 1, două numere pot să aibă și alte măsuri comune. De exemplu, 6 și 20 au ca măsură comună numărul 2: ambele sînt divizibile prin 2.

În general, orice număr prin care se împart fără rest două numere date este o măsură comună a lor. De aceea, se pune în mod firesc problema aflării tuturor divizorilor comuni a două numere date și, în particular, problema găsirii celui mai mare dintre divizorii lor comuni.

Se numește *cel mai mare divizor comun* a două numere date cel mai mare număr prin care sînt divizibile acestea. Dacă cel mai mare divizor comun a două numere este egal cu 1, se spune că aceste numere sînt *prime între ele*. De exemplu 8 și 9 sînt prime între ele. Tot astfel, vor fi prime între ele numerele 12 și 35. Iată definiția numerelor prime între ele, dată de Euclid: „Dacă dintre două numere întregi inegale cel mai mic se scade din cel mai mare și restul nu măsoară exact pe cel precedent pînă cînd el nu este egal cu unitatea, atunci numerele date sînt prime între ele”.

Acest fragment este foarte bogat în conținut. El nu dă numai definiția numerelor prime între ele, ci ne arată totodată cum să calculăm cel mai mare divizor comun. De aceea, după cum am mai spus, metoda pentru calculul celui mai mare divizor comun se numește *algoritm* lui Euclid.

Să exprimăm în limbajul actual al matematicii și să analizăm cu mai multă atenție această formulare foarte concisă a lui Euclid.

Fie date două numere naturale a și b , dintre care a este mai mare decît b ; trebuie să aflăm cel mai mare divizor comun al acestor numere. După Euclid ar urma să-l scădem pe cel mai mic din cel mai mare pînă cînd vom obține un rest; în loc să

procedăm astfel, vom împărți pe a prin b ; vom obține un cît m_1 și un rest r_1 , ceea ce se va putea scrie:

$$a = bm_1 + r_1 \quad (0 \leq r_1 < b).$$

Restul r_1 este mai mic decît b . Se poate întîmpla ca b să fie divizibil prin acest rest. Atunci membrul al doilea al egalității noastre, ca sumă a două numere divizibile prin r_1 , va fi de asemenea divizibil prin r_1 ; deci și numărul a , egal cu această sumă, va fi divizibil prin r_1 . Restul r_1 va fi divizorul comun al numerelor a și b . Pe de altă parte, scriind egalitatea sub forma $r_1 = a - bm_1$, vedem că orice divizor al numerelor a și b va fi divizor al numărului r_1 ; prin urmare, acest divizor nu va fi mai mare decît r_1 , ceea ce înseamnă că r_1 va fi cel mai mare divizor comun al numerelor a și b .

De exemplu, fie $a=24$ și $b=16$. Împărțind pe 24 prin 16, obținem cîtul 1 ($m_1=1$) și restul 8 ($r_1=8$). Însă 8 este divizor al lui 16. Înseamnă că 8 va fi cel mai mare divizor comun al numerelor 16 și 24. În adevăr, să verificăm. Iată toți divizorii numerelor 16 și 24:

Divizorii lui 16		1	2	4	8	16	
Divizorii lui 24	1	2	3	4	8	12	24
Divizorii comuni ai numerelor 16 și 24			1	2	4	8	

Cel mai mare dintre divizorii comuni ai numerelor 16 și 24 este numărul 8, pe care l-am obținut înainte.

Se poate întîmpla însă ca cel mai mic dintre numerele date b să nu se împartă prin r_1 . Înainte de a studia acest caz, atragem atenția asupra unui fapt important. Să admitem că la împărțirea prin b , numărul a dă restul r_1 . Am văzut că aceasta se scrie:

$$a = bn + r_1 \quad (0 < r_1 < b).$$

Orice divizor al numerelor a și b va fi divizor al lui r_1 sau, cu alte cuvinte, orice divizor comun al perechii de numere a și b va fi totodată un divizor al perechii b și r_1 ; prin urmare, cel mai mare divizor comun al numerelor a și b va fi totodată cel mai mare divizor comun al numerelor b și r_1 . Rezultă o teoremă importantă referitoare la aceasta.

Teoremă. Cel mai mare divizor comun a două numere este egal cu cel mai mare divizor comun al numărului mai mic și al restului obținut în împărțirea celui mai mare dintre numerele date prin cel mai mic.

Înarmați cu această teoremă, să revenim la analiza cazului cînd împărțirea lui a prin b ne dă restul r_1 , prin care b nu este divizibil. Atunci, împărțind pe b prin r_1 vom găsi un al doilea cît m_2 și un al doilea rest r_2 . La aceasta se referă Euclid cînd vorbește despre aplicarea consecutivă a scăderii repetate (după formula împărțirii cu rest). Prin urmare, obținem două egalități:

$$a = m_1b + r_1 \quad (0 < r_1 < b),$$

$$b = m_2r_1 + r_2 \quad (0 < r_2 < r_1).$$

Noul rest r_2 va fi mai mic decît noul împărțitor, adică decît primul rest r_1 . Așadar, obținem un rezultat important: $r_2 < r_1$.

Vom aplica această metodă succesiv, așa cum ne sfătuiește Euclid. Împărțim pe r_1 prin r_2 . Obținem un nou cît m_3 și un nou rest r_3 , neapărat mai mic decît r_2 :

$$r_3 < r_2.$$

Se pune întrebarea: se va termina vreodată acest șir de operații succesive sau este posibilă repetarea lor infinită, cum se întîmplă uneori la aflarea măsurii comune a două segmente? Se observă ușor că, în acest caz, nu este posibilă o repetare infinită a șirului de operații.

În adevăr, am văzut că primul rest r_1 este mai mic decît b . Al doilea rest r_2 este mai mic decît r_1 și așa mai departe:

$$b > r_1 > r_2 > r_3 > r_4 \dots$$

Numerele $b, r_1, r_2, r_3, \dots$ sînt întregi și pozitive; fiecare dintre ele este cel puțin cu o unitate mai mic decît cel precedent, astfel că ele sînt toate distincte. Nu există însă prea multe numere întregi și pozitive, distincte, mai mici decît b : numărul lor este $b-1$. Prin urmare, mai devreme sau mai tîrziu, împărțirile cu rest se vor termina și ultima împărțire nu va mai avea rest.

Să notăm cu n numărul de împărțiri consecutive cu rest. Avem:

$$\text{prima împărțire: } a = m_1b + r_1 \quad (0 < r_1 < b);$$

$$\text{a doua împărțire: } b = m_2r_1 + r_2 \quad (0 < r_2 < r_1);$$

$$\text{a treia împărțire: } r_1 = m_3r_2 + r_3 \quad (0 < r_3 < r_2);$$

$$\dots \dots \dots$$

$$\text{a } n\text{-a împărțire: } r_{n-2} = m_{n-1}r_{n-1} + r_n \quad (0 < r_n < r_{n-1}).$$

Următoarea împărțire, a $(n+1)$ -a, se va efectua neapărat fără rest:

$$\text{a } (n+1)\text{-a împărțire: } r_{n-1} = r_nm_{n+1}.$$

Acum vom face uz de teorema referitoare la cel mai mare divizor comun (p. 54). Din prima egalitate se vede că cel mai mare divizor comun al numerelor a și b este egal cu cel mai mare divizor comun al numerelor b și r_1 . Însă, în virtutea celei de-a doua egalități, acest divizor este egal cu cel mai mare divizor comun al numerelor r_1 și r_2 . Așadar, cel mai mare divizor comun al numerelor a și b este egal cu cel mai mare divizor comun al numerelor r_1 și r_2 . Considerînd a treia egalitate, ne convingem că ultimul este egal cu cel mai mare divizor comun al numerelor r_2 și r_3 . Înaintînd succesiv pînă la egalitatea a n -a, ajungem la concluzia că cel mai mare divizor comun al numerelor a și b este egal cu cel mai mare divizor comun al numerelor r_{n-1} și r_n . Însă r_{n-1} se împarte fără rest prin r_n . Prin urmare, r_n este cel mai mare divizor comun al numerelor r_{n-1} și r_n , deci cel mai mare divizor comun al numerelor a și b . În consecință, algoritmul lui Euclid ne duce efectiv la rezultatul căutat.

Modul în care se scriu operațiile când se calculează practic cel mai mare divizor comun poate fi ilustrat prin următorul exemplu. Să aflăm cel mai mare divizor comun al numerelor $a=729$ și $b=522$.

Începem operația mai aproape de marginea din dreapta a hîrtiei :

$$\begin{array}{rcl}
 a = & \dots\dots\dots & \\
 & - & \\
 & & 729 \overline{)522} \quad \dots\dots\dots = b \\
 & & 522 1 \\
 & & 522 \overline{)207} \quad \dots\dots\dots = r_1 \\
 & & - \\
 & & 414 2 \\
 & & 207 \overline{)108} \quad \dots\dots\dots = r_2 \\
 & & - \\
 & & 108 1 \\
 & & 108 \overline{)99} \quad \dots\dots\dots = r_3 \\
 & & - \\
 & & 99 1 \\
 & & 99 \overline{)9} \quad \dots\dots\dots = r_4 \\
 & & - \\
 & & 99 11
 \end{array}$$

În acest exemplu, împărțirea trebuie efectuată de $n+1=5$ ori. Al patrulea rest ($r_4=9$) este tocmai cel mai mare divizor comun al numerelor 729 și 522.

La aflarea celui mai mare divizor comun a două numere ne interesează numai resturile obținute din diversele operații de împărțire consecutive. Citurile nu ne interesează. De aceea, resturile din exemplul de mai sus au fost tipărite cu caractere grase. În unele probleme însă sînt importante citurile succesive; de aceste probleme nu ne vom ocupa aici¹⁾.

Să revenim la coloana de egalități scrise la aflarea celui mai mare divizor comun:

$$a = bm_1 + r_1;$$

$$b = r_1 m_2 + r_2;$$

$$r_1 = r_2 m_3 + r_3;$$

• • • • •

$$r_{n-3} = r_{n-2}m_{n-1} + r_{n-1};$$

$$r_{n-2} = r_{n-1}m_n + r_n.$$

În care a și b sînt cele două numere date (a este mai mare decît b), $m_1, m_2, \dots$ sînt cîturile succesive, iar $r_1, r_2, \dots$ resturile succesive.

Transcriem „pe dos“ această coloană, adică începînd cu ultima egalitate și rezolvăm în raport cu termenul din extrema dreaptă; obținem :

$$r_n = r_{n-2} - r_{n-1}m_n; \quad (1)$$

$$r_{n-1} = r_{n-3} - r_{n-2}m_{n-1}; \quad (2)$$

• • • • •

$$r_3 = r_1 - r_2 m_3; \quad (n-2)$$

$$r_2 = b - r_1 m_2; \quad (n-1)$$

$$r_1 = a - bm_1. \quad (n)$$

În dreapta este indicat numărul de ordine al fiecăreia dintre egalități. Să introducem acum în egalitatea (1) expresia lui r_{n-1} din egalitatea (2); obținem:

$$r_n = r_{n-2} - (r_{n-3} - r_{n-2}m_{n-1})m_n$$

sau

$$r_n = (1 + m_{n-1}m_n)r_{n-2} - m_nr_{n-3}.$$

Ultimul rest r_n , care este cel mai mare divizor comun al numerelor a și b , se exprimă prin numerele r_{n-2} și r_{n-3} , coeficienții

¹⁾ Citurile succesive sînt necesare, de exemplu, la dezvoltarea unui număr dat în fracție continuă, unde se aplică tot algoritmul lui Euclid.

lui r_{n-2} și r_{n-3} din această expresie fiind numere întregi (pozitive sau negative). Să notăm aceste numere cu A_1 și B_1 .
Avem:

$$A_1 = 1 + m_{n-1}m_n;$$

$$B_1 = -m_n.$$

Cu aceste notații, ultima egalitate se va scrie:

$$r_n = A_1 r_{n-2} + B_1 r_{n-3}.$$

Trecem acum la egalitatea (3) (ea nu a fost scrisă, ci înlocuită cu puncte, însă cititorul o poate reconstitui cu ușurință). Această egalitate exprimă pe r_{n-2} în funcție de r_{n-3} și r_{n-4} . Substituind-o în expresia lui r_n și reducând termenii asemenea, obținem:

$$r_n = A_2 r_{n-3} + B_2 r_{n-4},$$

unde A_2 și B_2 sînt iarăși numere întregi (pozitive sau negative). Repetînd operația de n ori, ajungem în sfîrșit la relația:

$$r_n = Aa + Bb. \quad (I)$$

Această relație dă cel mai mare divizor comun r_n a două numere întregi arbitrare a și b , în funcție de însăși numerele în cauză, coeficienții A și B fiind numere întregi.

Expresia (I) joacă un rol foarte important în teoria numerelor și o vom mai întîlni de repetate ori în cartea noastră.

Iată o primă aplicație a ei.

Să considerăm două numere a și m , prime între ele. Să presupunem că produsul ab al numărului dat a cu un număr întreg b este divizibil prin m . Ce putem spune despre divizibilitatea lui b prin m ?

Să aplicăm proprietatea celui mai mare divizor comun a două numere, exprimată de formula (I), coeficienții A și B fiind numere întregi (pozitive sau negative). Vom avea:

$$1 = Aa + Bm,$$

r_n fiind în cazul nostru egal cu unitatea, deoarece a și m sînt prime între ele.

Înmulțind ambii membri ai egalității cu b , rezultă

$$b = Aab + Bmb.$$

Cei doi termeni din membrul al doilea se divid prin m ; primul pentru că ab este divizibil prin m (conform ipotezei), iar al doilea, deoarece conține explicit factorul m . Prin urmare, și membrul întîi, adică numărul b este divizibil prin m .

În felul acesta am obținut demonstrația celei de-a treia teoreme considerate la începutul acestui capitol (p. 50).

Am mai întîlnit o împărțire consecutivă — de natură întrucîtva diferită — la convertirea unui număr dintr-un sistem de numerație în altul (p. 34). Acolo, spre deosebire de algoritmul lui Euclid, toți divizorii erau identici. Să insistăm ceva mai amănunțit asupra acestei împărțiri.

Fie date un număr a și o bază m a unui sistem de numerație. Numărul a poate fi dat în orice alt sistem de numerație, scris cu cifre romane sau într-un alt mod. Se pune problema principală: poate fi oare numărul a scris în sistemul pozițional cu baza m ? Am văzut cum decurge practic aceasta; toate exemplele întîlnite în capitolele IV și V par să confirme această posibilitate. Mai rămîne să studiem problema din punct de vedere teoretic, adică să demonstrăm teorema sub forma ei generală.

Așadar, se cere ca numărul a să fie scris în sistemul cu baza m . Împărțim pe a prin m . După cum știm, aceasta revine la determinarea în mod unic a cîtului n_1 și restului r_1 :

$$a = mn_1 + r_1.$$

n_1 arată cîte grupe de m unități (cîte unități de ordinul al doilea) sînt conținute în numărul a . r_1 dă numărul de unități libere de primul ordin. Dacă numărul n_1 este mai mic decît baza sistemului de numerație, problema este rezolvată: numărul nostru este format din n_1 unități de ordinul al doilea și din r_1 unități de ordinul întîi și se scrie:

$$n_1 r_1^1).$$

Dacă însă n_1 este mai mare decît m , repetăm aceeași operație: împărțim pe n_1 prin m și obținem cîtul n_2 și restul r_2 . Cîtul reprezintă numărul de unități de ordinul al treilea, iar restul, numărul de unități de ordinul al doilea. Dacă n_2 este mai mic decît m ,

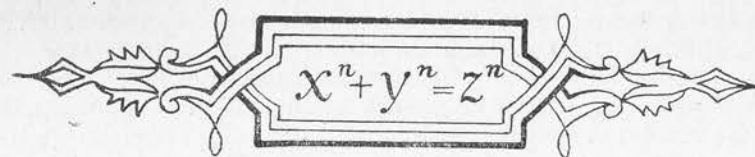
¹⁾ Aici, ca și în capitolul IV (v. p. 34), $n_1 r_1$ nu înseamnă produsul numerelor n_1 și r_1 , ci doar două cifre scrise alături, cum sînt cifrele 3 și 5 în numărul 35.

problema este rezolvată, în sensul că numărul a se scrie în sistemul cu baza m astfel :

$$n_2 r_2 r_1$$

(adică $n_2 m^2 + r_2 m + r_1$). În cazul cînd n_2 este mai mare decît m , repetăm împărțirea.

Însă numărul a este un număr dat, perfect determinat. Dacă vom considera șirul de puteri ale numărului întreg m , mai mare decît 1, adică $m, m^2, m^3, \dots$, atunci vom găsi neapărat în acest șir o putere cu un anumit exponent (să-l notăm cu q), astfel încît m^q să fie mai mare decît a . Așadar, după q împărțiri succesive prin m , operația se va încheia și vom obține o reprezentare unică, bine determinată, a numărului a în sistemul pozițional cu baza m . Este tocmai ceea ce voiam să demonstrăm.



CAPITOLUL VII

ECUAȚIILE PE CARE LE STUDIAZĂ ARITMETICA



Titlul acestui capitol poate trezi nedumeriri : în adevăr, ecuațiile se studiază în algebră ! Care pot fi atunci ecuațiile ce intră în preocupările aritmeticii ? Se constată că există un tip special de ecuații — mai exact un punct de vedere deosebit asupra unor ecuații — care, prin esența sa, este mult mai aproape de aritmetică decît de algebră. Despre ce fel de ecuații este vorba ?

Să luăm următoarea problemă simplă.

Într-un artel era un anumit număr de muncitori calificați și necalificați. Fiecare muncitor calificat a primit pentru munca efectuată cîte 210 ruble, iar fiecare muncitor necalificat, cîte 150 ruble. În total, s-au încasat 1 740 ruble. Cîți lucrători calificați avea artelul și cîți necalificați ?

Ecuația acestei probleme este foarte ușor de alcătuit : dacă numărul muncitorilor calificați este x , iar al celor necalificați y , atunci primii au cîștigat $210x$ ruble, iar ceilalți $150y$ ruble. Suma acestor cantități trebuie să fie egală cu cîștigul total, ceea ce dă imediat ecuația

$$210x + 150y = 1\,740$$

sau, după simplificarea cu 30 :

$$7x + 5y = 58.$$

Aici intervine însă o dificultate : nu dispunem de nici un fel de date pentru întocmirea celei de-a doua ecuații. În astfel de probleme, care se găsesc în număr foarte mare în diferite culegeri, se dă întotdeauna cîte o condiție suplimentară : fie numărul total

al muncitorilor, fie raportul dintre numărul de muncitori calificați și necalificați, fie altceva asemănător. Atunci putem scrie o a doua ecuație și rezolva fără dificultate sistemul simplu pe care l-am obținut. În exemplul nostru nu avem date suplimentare. Trebuie rezolvată ecuația unică:

$$7x + 5y = 58.$$

Din punctul de vedere al algebrei, problema este clară: ecuația are o infinitate de soluții. Oricărui număr x , arbitrar, îi corespunde un număr y determinat, pe care îl calculăm cu formula

$$y = \frac{58 - 7x}{5}.$$

Această soluție a problemei nu ne poate însă satisface. În adevăr, numărul de muncitori din fiecare categorie trebuie să fie întreg și pozitiv (în caz extrem, una dintre necunoscute poate fi egală cu zero, artelul fiind format din lucrători dintr-o singură categorie).

Așadar, din infinitatea de soluții ale ecuației $7x + 5y = 58$ ne interesează numai perechile de valori pentru x și y în care ambele necunoscute sînt numere naturale. Se vede ușor că pentru $x = 0$ sau $y = 0$, a doua necunoscută este fracționară, astfel că putem lăsa de o parte soluțiile nule. Aceasta ne va permite să separăm o anumită soluție determinată și să rezolvăm problema pînă la capăt.

Vom da necunoscutei x valori întregi și vom calcula valorile corespunzătoare ale lui y . Nu va trebui să facem prea multe încercări, deoarece pentru $x > 8$, a doua necunoscută devine negativă și deci nu ne interesează. Să formăm tabela

x	0	1	2	3	4	5	6	7	8
$y = \frac{58 - 7x}{5}$	$\frac{58}{5}$	$\frac{51}{5}$	$\frac{44}{5}$	$\frac{37}{5}$	6	$\frac{23}{5}$	$\frac{16}{5}$	$\frac{9}{5}$	$\frac{2}{5}$

Observăm că singura valoare întreagă și pozitivă a lui y ($y = 6$) se obține pentru $x = 4$. Pentru orice alte valori ale lui x , numărul y este ori fracționar, ori negativ. Prin urmare, problema are o soluție unică și pe deplin determinată: în artel erau 4 muncitori calificați și 6 muncitori necalificați.

Condiția suplimentară, ca soluția să fie în numere întregi și pozitive, ne-a ținut loc de a doua ecuație.

Problema studiată mai sus a dus la o ecuație cu două necunoscute. Sînt însă posibile și probleme în care o singură ecuație leagă mai mult decît două necunoscute sau probleme care conduc la sisteme cu un număr de ecuații mai mic decît cel al necunoscutelor. Astfel de ecuații sau sisteme de ecuații se numesc nedeterminate, deoarece, dacă nu dispunem de condiții suplimentare, ele au o infinitate de soluții: putem da valori oarecare uneia sau mai multora dintre necunoscute și atunci valorile celorlalte necunoscute sînt determinate. Ecuațiile nedeterminate, cu infinitatea lor de soluții, sînt foarte utile în matematica superioară, la studiul curbilor și al suprafețelor.

Situația se prezintă altfel cînd mărimile căutate trebuie să satisfacă, pe lîngă ecuația nedeterminată, și unele condiții suplimentare. Cazul cel mai important și mai bine studiat este acela cînd se caută soluții întregi, așa cum era situația din exemplul anterior. De cele mai multe ori se caută toate soluțiile întregi, pozitive și negative. Alteori, se impun soluției condiții restrictive mult mai severe.

Acest gen de cercetare a ecuațiilor nedeterminate se numește analiză nedeterminată sau analiză diofantiană după numele celebrului matematician elin Diofant care a trăit la Alexandria în secolul III al erei noastre (aceasta este tot ce se știe despre viața lui). Diofant a scris o carte din care au învățat creatorii teoriei moderne a numerelor. Trebuie relevat că el a căutat nu numai rădăcinile întregi ale ecuațiilor nedeterminate, ci și pe cele raționale (adică rădăcinile întregi și fracționare). Mult mai tîrziu, indienii au început să se ocupe de rezolvarea în numere întregi a ecuațiilor nedeterminate și de discutarea rezultatelor obținute. De altfel este greu de spus cînd a apărut pentru prima dată analiza nedeterminată. În orice caz, în secolul al XII-lea e.n. matematicianul indian Bhāskara avea o metodă perfect elaborată pentru rezolvarea ecuațiilor nedeterminate de gradul întâi în numere întregi.

Indienii au fost puși în situația de a rezolva unele probleme din practică cu ajutorul analizei nedeterminate.

Astfel, în legătură cu calendarul, ei au fost adeseori nevoiți să găsească un interval de timp conținînd atît un număr întreg de ani, cît și un număr întreg de zile. Aceasta ducea la ecuații nedeterminate; numai soluțiile întregi ale acestor ecuații prezentau interes.

Să studiem câteva probleme cu ecuații nedeterminate, pentru a ne da seama de principalele lor particularități. Ne vom mărgini la ecuațiile de gradul întâi, deoarece rezolvarea ecuațiilor nedeterminate de grad superior, chiar numai de gradul al doilea, prezintă dificultăți considerabile.

Problema întâi. *Se cere să schimbăm o bancnotă de 5 ruble în monede de câte 50, 20 și 5 copeici, astfel ca numărul total de monede să fie 20.*

Scriem ecuația problemei. Fie x numărul de monede de câte 5 copeici, y numărul de monede de câte 20 de copeici; z numărul de monede de câte 50 copeici. Suma totală, egală cu 500 copeici, se va exprima astfel: $5x + 20y + 50z$; pe de altă parte, prin ipoteză, avem $x + y + z = 20$. Alte date nu mai există. Prin urmare, trebuie rezolvat în numere întregi sistemul:

$$5x + 20y + 50z = 500$$

$$x + y + z = 20.$$

Numărul de necunoscute este mai mare decât numărul de ecuații, deci sistemul de ecuații este nedeterminat. Simplificînd prima ecuație cu 5 și scăzînd din ea a doua, obținem o singură ecuație cu două necunoscute:

$$3y + 9z = 80.$$

Urmează să rezolvăm această ecuație în numere întregi. Examinînd-o cu mai multă atenție, observăm că, oricare ar fi valorile întregi ale lui y și z , membrul întâi al ecuației trebuie să fie divizibil prin 3. În schimb, membrul al doilea nu este divizibil prin 3. Așadar, nu există valori întregi ale lui y și z care să satisfacă ecuația noastră. Acesta este un exemplu de ecuație nedeterminată care nu poate fi rezolvată în numere întregi. Prin urmare, nici problema care ne-a condus la această ecuație nu are soluție. Este imposibil să schimbăm o bancnotă de 5 ruble în 20 de monede cu valorile indicate.

Problema a doua. *Să se afle ce număr natural împărțit prin 3 dă restul 2, iar împărțit prin 5 dă restul 3.*

Notăm cu x numărul căutat. Dacă vom nota cu y cîtuș împărțirii lui x prin 3 și cu z cîtuș împărțirii lui x prin 5, vom avea (v. p. 50):

$$x = 3y + 2$$

$$x = 5z + 3.$$

Conform sensului problemei, x , y și z trebuie să fie numere întregi (mai mult chiar, numere naturale). Așadar, aici de asemenea tre-

buie să rezolvăm în numere întregi un sistem de ecuații nedeterminat.

Găsirea numărului x nu prezintă dificultăți. Oricare ar fi numerele întregi y și z , x va fi de asemenea întreg. De aceea trebuie să rezolvăm următoarea ecuație cu două necunoscute:

$$5z - 3y + 1 = 0.$$

Determinînd toate valorile întregi și pozitive ale lui y sau z , putem obține imediat și toate valorile întregi și pozitive ale lui x .

Din ecuația $5z - 3y + 1 = 0$, obținem

$$y = \frac{5z + 1}{3}$$

O soluție este evidentă: pentru $z = 1$, obținem

$$y = \frac{5 \cdot 1 + 1}{3} = 2.$$

Pentru aceste valori ale lui z și y întregi corespunde $x = 8$, de asemenea întreg.

Să găsim toate celelalte soluții întregi și pozitive, care corespund valorilor lui y și z întregi și pozitive. Vom introduce necunoscuta auxiliară u , punînd $z = 1 + u$. Avem

$$5(1 + u) - 3y + 1 = 0$$

adică

$$5u = 3y - 6$$

sau

$$5u = 3(y - 2).$$

Membrul al doilea al ultimei ecuații este divizibil prin 3, pentru orice y întreg. Prin urmare, și membrul întâi trebuie să fie divizibil prin 3. Numerele 5 și 3 sînt însă prime între ele; deci trebuie ca u să fie divizibil prin 3¹⁾, adică să fie de forma $3n$, unde n este un număr întreg. În acest caz, y va fi egal cu

$$\frac{15n}{3} + 2 = 5n + 2,$$

adică tot cu un număr întreg. Așadar

$$z = 1 + u = 1 + 3n$$

de unde

$$x = 5z + 3 = 8 + 15n.$$

¹⁾ Vezi teorema a treia din capitolul precedent (p. 50).

Am obținut pentru x o infinitate de valori, iar soluțiile problemei noastre sînt de forma:

$$x = 8 + 15n,$$

unde n este un număr întreg (pozitiv sau nul)

$$n = 0, 1, 2, 3, \dots$$

Verificarea arată că toate aceste soluții sînt bune.¹⁾

Problema a treia. *Un cetățean a cumpărat pepeni galbeni cu 7 ruble bucata și pepeni verzi cu 4 ruble bucata. În total a plătit 53 ruble. Cîți pepeni galbeni și cîți pepeni verzi i-au revenit?*

O ecuația se scrie imediat:

$$7x + 4y = 53,$$

în care x este numărul de pepeni galbeni și y numărul de pepeni verzi.

Problema nu are sens decît dacă x și y sînt simultan numere întregi și pozitive. Să o rezolvăm în acest sens. Mai întîi avem:

$$y = \frac{53 - 7x}{4}$$

Dăm lui x valori începînd cu 1; constatăm că pentru $x > 7$, y ia valori negative. Ne oprim deci la 7 și calculăm valorile corespunzătoare ale lui y cînd $x = 1, \dots, 7$:

x	1	2	3	4	5	6	7
$y = \frac{53 - 7x}{4}$	$11\frac{1}{2}$	$9\frac{3}{4}$	8	$6\frac{1}{4}$	$4\frac{1}{2}$	$2\frac{3}{4}$	1

Singurele soluții întregi și pozitive ale problemei sînt:

$$1) \begin{cases} x=3 \\ y=8 \end{cases} \quad \text{și} \quad 2) \begin{cases} x=7 \\ y=1. \end{cases}$$

În toate celelalte cazuri, cel puțin una dintre necunoscute este fracționară, fără a mai vorbi de valorile negative. Prin urmare, problema are două soluții: ori s-au cumpărat 3 pepeni galbeni

¹⁾ Toate soluțiile acestei probleme formează o progresie aritmetică infinită, în care primul termen este 8, iar rația $15 : \div 8, 23, 38, 53, 68, 83, \dots$

și 8 pepeni verzi (ceea ce costă $3 \cdot 7 + 8 \cdot 4 = 53$ ruble), ori 7 pepeni galbeni și un pepene verde (ceea ce revine la $7 \cdot 7 + 1 \cdot 4$, adică iarăși 53 ruble).

Așadar, în problemele care conduc la ecuații nedeterminate întîlnim situațiile cele mai variate: problema poate fi cu totul nerezolvabilă, poate avea o infinitate de soluții, poate avea cîteva soluții pe deplin determinate și, în particular, ea poate avea o soluție unică.

Să menționăm deosebirea în ceea ce privește rezolvarea unei ecuații în algebră și rezolvarea în analiza diofantiană. În algebră domină tendința de a rezolva ecuația în cazul cel mai general, de a-i găsi toate soluțiile posibile. Pentru ca ecuațiile algebrice să fie rezolvabile în toate cazurile, a fost necesară introducerea numerelor iraționale și complexe. Analiza nedeterminată însă se bazează numai pe soluțiile în numere întregi. Ce e drept, în analiza nedeterminată nu putem renunța la numerele negative, deoarece folosirea lor ne permite să obținem formule generale foarte comode, fără a considera prea multe cazuri particulare. Întrucît analiza nedeterminată consideră numai soluțiile întregi, putem utiliza pentru aflarea lor proprietățile numerelor întregi: divizibilitatea, descompunerea în factori primi, aflarea celui mai mare divizor comun etc. Acestea sînt noțiuni din domeniul aritmeticii, nu din acela al algebrei. De aceea, analiza nedeterminată este considerată de obicei un capitol al aritmeticii și nu un capitol al algebrei. Astfel, titlul capitolului de față este justificat.

Să trecem la studiul mai atent al unei ecuații nedeterminate de gradul întîi cu două necunoscute. După „prelucrarea” obișnuită la care supunem în general o ecuație (eliminarea numitorilor, reducerea termenilor asemenea etc.), ea poate fi scrisă:

$$ax + by = c. \quad (I)$$

Aici a, b, c sînt numere întregi (pozitive sau negative) date, iar x și y sînt necunoscutele, care iau numai valori întregi (de asemenea pozitive, negative sau nule).

Să considerăm întîi cazul cînd ecuația nedeterminată nu are soluție (ca în problema întîi, p. 64).

Să aflăm cel mai mare divizor comun al numerelor a și b . Îl notăm cu d (dacă a și b sînt prime între ele, d este egal cu 1). Atunci a va fi egal cu produsul dintre d și un număr întreg m , iar b va fi egal cu produsul lui d cu un alt număr întreg n :

$$a = md, \quad b = nd.$$

m și n din aceste relații vor fi neapărat prime între ele. În adevăr, dacă ele ar avea un divizor comun k , diferit de 1, produ-

sul kd ar fi divizor atât al numărului a , cât și al numărului b , astfel că d nu ar fi cel mai mare divizor comun al acestor două numere.

Membrul întâi al ecuației (I) trebuie să fie divizibil prin d , oricare ar fi numerele întregi x și y , deoarece ambii termeni ax și by sînt multipli de d . Așadar, membrul al doilea al acestei ecuații trebuie să se împartă prin d . De aici putem trage următoarea concluzie: dacă termenul liber al unei ecuații nedeterminate nu este divizibil prin cel mai mare divizor comun al coeficienților necunoscutelor, atunci ecuația (I) este imposibilă. În problema întâi (v. p. 64), am ajuns la ecuația

$$3y + 9z = 80;$$

aici cel mai mare divizor comun al coeficienților este egal cu 3, iar termenul liber nu este un multiplu de 3; prin urmare, ecuația nu are soluție. Când am studiat această problemă am văzut că, într-adevăr, ea nu are soluție.

Dacă se dă ecuația nedeterminată (I), trebuie să vedem mai întâi dacă nu se încadrează în cazul analizat. Dacă se încadrează, atunci ecuația nu poate avea soluție în numere întregi și deci nu ne interesează. Așadar, merită a fi studiate numai ecuațiile în care toți termenii sînt divizibili prin cel mai mare divizor comun al coeficienților necunoscutelor. Toți termenii unei asemenea ecuații pot fi împărțiți cu acest divizor și se obține o ecuație în care coeficienții necunoscutelor sînt numere prime între ele. De aceea, în raționamentele care urmează, vom considera că în ecuația

$$ax + by = c \quad (I)$$

numerele a și b nu vor fi numai întregi, ci și prime între ele. Ecuațiile de gradul întâi se numesc și ecuații liniare¹⁾. Ecuațiile în care toți termenii au același grad, adică suma exponenților necunoscutelor, dintr-un termen (monom) este egală cu suma corespunzătoare din fiecare alt termen se numesc omogene. De exemplu, ecuațiile $x^2 + 2xy = y^2$ sau $x^3 + y^3 = 3xy^2$ sînt omogene. Ecuațiile omogene au multe proprietăți interesante și se rezolvă, de obicei, mai simplu decît cele neomogene. În cazul

¹⁾ Această denumire se explică prin faptul că, în geometria analitică (știința cu care se începe de obicei studiul matematicii superioare), ecuația $ax + by = c$ reprezintă o linie dreaptă.

ecuațiilor liniare, este omogenă ecuația fără termen liber, acesta fiind de grad zero. De exemplu ecuațiile

$$2x + 3y = 0; \quad x - 3y = 2z; \quad x - y = u - v$$

sînt omogene; în schimb ecuațiile

$$2x + 3y = 5; \quad x - 3y + 1 = 2z; \quad x - y = u - v + 100$$

sînt neomogene.

Ca prim exemplu să considerăm următoarele două ecuații:

$$2x + 3y = 5; \quad 2x + 3y = 0.$$

Aceste ecuații au aceiași coeficienți ai necunoscutelor. Se spune că a doua ecuație este ecuația omogenă corespunzătoare primei ecuații (neomogene). Studiind ecuația liniară nedeterminată $ax + by = c$, este firesc să începem prin a considera ecuația omogenă, adică să punem $c = 0$:

$$ax + by = 0.$$

Putem scrie această ecuație mai comod astfel:

$$ax = by^1).$$

Rezolvarea ei este foarte simplă. Membrul al doilea by este divizibil prin b , ceea ce înseamnă că și membrul întâi ax trebuie să fie divizibil prin b . Numerele a și b sînt însă prime între ele; prin urmare este absolut necesar ca x să fie multiplu de b (v. a treia teoremă din capitolul precedent).

Așadar

$$x = bn.$$

Pentru a-l găsi pe y , introducem expresia lui x în ecuația $ax = by$. Obținem:

$$abn = by,$$

de unde

$$y = an.$$

n trebuie să fie în mod obligator același ca și în expresia lui x .

Prin urmare, soluția ecuației omogene este de forma:

$$\left. \begin{array}{l} x = bn \\ y = an \end{array} \right\} \quad (II)$$

unde n este un întreg arbitrar. Reciproc, pentru orice n întreg, valorile lui x și y vor fi întregi și vor transforma ecuația dată

¹⁾ Cititorul va fi, eventual, șocat că am scris $ax = by$ în loc de $ax = -by$. În fond, aici întâi am scris $ax = -by$, apoi am pus $b_1 = -b$, ceea ce dă $ax = b_1 y$; în sfîrșit, b_1 reprezentînd un număr cu totul arbitrar, l-am înlocuit cu litera b .

într-o identitate. Prin urmare, formulele (II) rezolvă complet ecuația omogenă.

Problemele care i-au condus pentru prima oară pe astronomii indieni la ecuații nedeterminate (v. p. 64) se exprimau tocmai prin ecuații omogene.

În tehnica modernă avem adeseori de-a face cu ecuații omogene nedeterminate. Ca exemplu vom da următoarea problemă referitoare la numărul de dinți ai roților din angrenaje. Pentru funcționarea lină a unei transmisii cu roți dințate este necesar ca numărul de dinți corespunzător unei roți și numărul corespunzător celei de a doua să fie în același raport ca și numerele de rotații ale celor două roți, în unitatea de timp. De exemplu dacă prima dintre roți are turația 50 rot/min, iar a doua turația 80 rot/min, atunci numărul x al dinților primei roți și numărul de dinți y al celei de-a doua trebuie să fie în același raport ca și 80 cu 50; prin urmare, avem:

$$\frac{x}{y} = \frac{80}{50} \quad \text{sau} \quad 5x = 8y.$$

Am obținut o ecuație omogenă, care se rezolvă ușor în numere întregi. Conform cu formulele (II), avem:

$$x = 8n, \quad y = 5n,$$

unde n este un întreg arbitrar.

Trecem acum la ecuațiile nedeterminate neomogene de gradul întâi, adică la ecuațiile de forma:

$$ax + by = c.$$

După cum vom vedea, toate soluțiile unei astfel de ecuații se pot scrie prin două formule care conțin un număr întreg arbitrar n [analog cu formulele (II) în cazul ecuației omogene]. Aceste formule reprezintă soluția generală a ecuației (I), iar fiecare pereche de valori ale necunoscutelor, pe care o vom obține alegând o anumită valoare pentru n , va fi o soluție particulară. În ecuația omogenă $5x = 8y$, soluția

$$x = 8n, \quad y = 5n$$

va fi generală, iar soluția

$$x = 24, \quad y = 15,$$

obținută din cea precedentă pentru $n=3$, va fi o soluție particulară.

Să presupunem că, prin încercări, am izbutit să determinăm o soluție particulară a ecuației $ax + by = c$, cu alte cuvinte am găsit două numere întregi x_0 și y_0 care satisfac relația:

$$ax_0 + by_0 = c.$$

Să aplicăm procedeul utilizat în algebră, anume, să introducem două necunoscute auxiliare u și v , legate de vechile necunoscute x și y prin relațiile:

$$x = x_0 + u \quad y = y_0 + v.$$

Substituind aceste expresii în ecuația $ax + by = c$, obținem:

$$a(x_0 + u) + b(y_0 + v) = c.$$

Desfacem parantezele și regrupăm termenii; rezultă:

$$ax_0 + by_0 + au + bv = c.$$

Scăzând din această egalitate identitatea $ax_0 + by_0 = c$, vom avea:

$$au + bv = 0 \quad \text{sau} \quad au = -bv.$$

Aceasta este ecuația omogenă corespunzătoare ecuației neomogene $ax + by = c$. Soluția ei poate fi scrisă imediat, conform relațiilor (II):

$$\left. \begin{aligned} u &= -bn, \\ v &= an. \end{aligned} \right\} ^1)$$

Prin urmare

$$x = x_0 + u = x_0 - bn$$

$$y = y_0 + v = y_0 + an.$$

Aceasta este forma pe care trebuie s-o aibă orice soluție a ecuației $ax + by = c$. Pe de altă parte, substituind valorile lui x și y în ecuația (I), ne convingem că aceasta va fi satisfăcută, oricare ar fi n . În adevăr,

$$a(x_0 - bn) + b(y_0 + an) = ax_0 + by_0,$$

iar acest număr este egal cu c , deoarece x_0 și y_0 satisfac ecuația (I).

Prin urmare, am obținut soluția generală a ecuației neomogene.

¹⁾ Aici avem semnul „minus” înaintea lui b , care nu figura în formulele (II), deoarece ecuația considerată este de forma $au = -bv$ și nu $au = bv$; deci coeficientul lui b este precedat de un „minus”.

În felul acesta am ajuns la un rezultat remarcabil: soluția generală a unei ecuații liniare neomogene este egală cu suma soluției particulare și soluției generale a ecuației omogene corespunzătoare. Acest rezultat este simplu, însă foarte important. Este de ajuns să menționăm că teoreme analoge se întâlnesc în cele mai diferite capitole ale matematicii superioare.

Se pune întrebarea: cum găsim numerele x_0 și y_0 , deci cum găsim cel puțin o singură soluție a ecuației nedeterminate (I)? Dacă coeficienții a , b și c ai acestei ecuații nu sînt mari, este cel mai bine să alegem această soluție în modul următor: dăm uneia dintre necunoscute, de exemplu lui x , consecutiv valorile 0, 1, 2, 3, ..., pînă cînd vom obține o valoare întregă pentru a doua necunoscută y . Acest procedeu a fost utilizat la rezolvarea problemei a treia (p. 66). Dacă însă coeficienții a , b și c sînt mari, trebuie să recurgem la algoritmul lui Euclid. Indienii din antichitate au procedat asemănător; tot așa procedează și matematicienii contemporani. Modul în care se aplică algoritmul lui Euclid la rezolvarea ecuației (I) îl vom ilustra printr-un exemplu numeric.

Să se rezolve ecuația:

$$331x - 169y = 5.$$

Căutăm întîi o soluție particulară.

Prima operație pe care ne vom strădui să o facem va fi micșorarea coeficienților ecuației. În acest scop, împărțim coeficientul mai mare (331) prin cel mai mic (169). Obținem citul 1 și restul 162. Așadar,

$$331 = 169 + 162 \quad \text{sau} \quad 331x = 169x + 162x.$$

Ecuația se poate scrie acum:

$$162x + 169x - 169y = 5 \quad \text{sau} \quad 162x + 169(x - y) = 5.$$

Să recurgem iarăși la introducerea de necunoscute auxiliare. Vom lua ca nouă necunoscută pe:

$$z = x - y. \quad (1)$$

Obținem ecuația cu coeficienți mai mici:

$$162x + 169z = 5.$$

Observăm că în egalitatea (1), care leagă pe z de vechile necunoscute x și y , necunoscuta auxiliară z intervine cu coefi-

cientul 1. Aceeași remarcă se poate face și în ceea ce privește necunoscuta y , care intervenea în ecuația inițială cu un coeficient mai mic în valoare absolută.

Aplicăm același procedeu și ecuației obținute: împărțim coeficientul mai mare prin cel mai mic, cu alte cuvinte, *împărțim coeficientul mai mic al ecuației inițiale* (169) *prin primul rest* (162). Obținem citul 1 și restul 7, adică $169z = 162z + 7z$. Ecuația inițială se scrie acum:

$$7z + 162z + 162x = 5 \quad \text{sau} \quad 162(x + z) + 7z = 5.$$

Introducem o nouă necunoscută auxiliară:

$$u = x + z. \quad (2)$$

[Atragem atenția că în ecuația (2), atît u (noua necunoscută) cît și x (vechea necunoscută, care avea coeficientul mai mic în ecuația precedentă), au coeficientul 1!]

Obținem:

$$162u + 7z = 5.$$

Împărțim iarăși coeficientul mai mare prin cel mai mic, adică *împărțim primul rest al ecuației inițiale* (162) *prin al doilea rest* (7); obținem citul 23 și restul 1. Prin urmare, $162u = 7 \cdot 23u + u$ și ecuația devine

$$u + 7 \cdot 23u + 7z = 5 \quad \text{sau} \quad u + 7(23u + z) = 5.$$

Introducem o ultimă necunoscută auxiliară:

$$v = 23u + z. \quad (3)$$

(Și aici noua necunoscută v și vechea necunoscută z , adică aceea care intra cu coeficientul mai mic în ecuația precedentă, au coeficientul 1. Situația va fi întotdeauna aceasta; cititorul poate demonstra singur această afirmație.)

Ecuația inițială a luat acum forma deosebit de simplă:

$$u + 7v = 5.$$

Ea este mai avantajoasă decît cele precedente, deoarece una dintre necunoscute are coeficientul 1. Aceasta nu este o întîmplare ce apare doar în exemplul nostru, ci o proprietate generală. În adevăr, revăzînd toate rîndurile raționamentului tipărite cu litere cursive, cititorul se va convinge că am calculat de fapt cel mai mare divizor comun al celor doi coeficienți ai necunoscutelor din

ecuația inițială, iar șirul de operații se va încheia atunci când unul dintre coeficienții ecuației respective va deveni egal cu acest divizor comun. Reamintim că ne ocupăm numai de ecuații în care coeficienții sînt numere prime între ele¹⁾. Prin urmare, cel mai mare divizor comun al lor este egal cu 1 și ultima dintre ecuațiile simplificate va avea neapărat unul dintre coeficienți egal cu unitatea.

Ultima ecuație ne dă:

$$u=5-7v.$$

Pentru orice v întreg, și u va fi întreg. Făcîndu-l pe v egal, de exemplu cu 0, obținem $u=5$. Acum vom urma raționamentul „de jos în sus”, parcurgînd toate egalitățile marcate cu numerele (3), (2), (1). Fiecare necunoscută ce urmează a fi determinată, va avea coeficientul 1 (am atras tot timpul atenția asupra acestui fapt!). De aceea toate necunoscutele (deci și x și y) vor fi numere întregi. În exemplul nostru obținem:

$$v=0;$$

$$u=5;$$

$$z=v-23u=-115;$$

$$x=u-z=5-(-115)=120;$$

$$y=x-z=120-(-115)=235.$$

Așadar, soluția particulară a ecuației este:

$$x_0=120, \quad y_0=235.$$

Știm deja cum se află soluția ei generală. În acest scop vom considera ecuația omogenă corespunzătoare:

$$331x-169y=0;$$

aici $a=331$, $b=169$. De aceea [v. formulele (II) la p. 69] soluția generală a ecuației neomogene $331x-169y=5$ va fi:

$$x=120+169n; \quad y=235+331n.$$

Această metodă de rezolvare este întrucîtva greoaie, însă merită să insistăm asupra ei din două motive; în primul rînd pune în evidență legătura dintre procedeul de rezolvare a unei ecuații nedeterminate și algoritmul lui Euclid; în al doilea rînd ea arată că ecuația are o soluție, oricare ar fi coeficienții necunos-

¹⁾ Dacă ele au un divizor comun diferit de 1, sau ecuația este nerezolvabilă sau ea poate fi simplificată cu acest factor.

cutelor primi între ei. În practică, acest procedeu nu se continuă pînă la capăt; după ce obținem o ecuație ajutătoare cu coeficienți relativ mici, rezolvăm această ecuație prin încercări. Insuși mer-sul rezolvării poate fi raționalizat. În acest caz, calculele vor fi simplificate, dar se va pierde din vedere esența problemei¹⁾.

Există formule pentru rezolvarea unei ecuații nedeterminate de gradul întii cu două necunoscute, însă deducerea și aplicarea lor se bazează pe folosirea fracțiilor continue, pe care cititorul, probabil, nu le cunoaște. Menționăm că teoria fracțiilor continue se leagă și ea de algoritmul lui Euclid, astfel că nici în acest caz nu ne putem lipsi de el.

Am mai arătat că prima carte consacrată ecuațiilor nedeterminate a fost scrisă de Diofant (sec. III e.n.). Avem motive să credem că, 500 de ani înaintea lui Diofant, Arhimede era în stare să rezolve astfel de ecuații. În Evul Mediu s-au ocupat de ele indienii și arabii. În Europa, primul care a început să studieze soluțiile în numere întregi ale ecuațiilor nedeterminate a fost matematicianul francez Bachet de Meziriac, editor și comentator al operelor lui Diofant (începutul secolului al XVII-lea).

Se știe că Diofant a considerat, alături de ecuațiile liniare (de gradul întii), și ecuațiile nedeterminate de gradul al doilea și al treilea. De regulă, rezolvarea lor este complicată. Să ne oprim asupra unei probleme devenite clasice.

Problema este următoarea: *să se afle triunghiurile drept-unghice ale căror laturi se exprimă toate prin numere întregi.*

Teorema lui Pitagora ne permite să scriem imediat ecuația acestei probleme. Dacă vom nota cu x și cu y lungimile catetelor și cu z lungimea ipotenuzei, vom avea:

$$x^2+y^2=z^2.$$

Aceasta este o ecuație nedeterminată cu trei necunoscute, omogenă și de gradul al doilea. Una dintre soluții este unanim cunoscută: catetele de 3 și 4 unități, iar ipotenuza de 5 unități („triunghiul egiptean”). Dar aceasta este o soluție particulară și cunoașterea ei ne-ar permite să rezolvăm complet ecuația numai dacă ar fi liniară. Pentru a obține însă soluția completă, în cazul de față va trebui să folosim un artificiu de calcul.

¹⁾ O astfel de metodă simplificată pentru rezolvarea unei ecuații nedeterminate este dată, de exemplu, în partea a doua a manualului de algebră a lui Kiseliiov și în cartea lui Я. Перельман, „Занимательная алгебра”, Гостехиздат, Москва, 1955.

Vom căuta trei numere x, y și z care satisfac ecuația lui Pitagora ¹⁾ și care nu au nici un factor comun în afară de 1 ²⁾. Este important să găsim tocmai aceste soluții, deoarece orice soluție formată din numerele prime între ele x_0, y_0 și z_0 conduce imediat la o serie de soluții formate din numere neprime între ele: nx_0, ny_0, nz_0 , unde n este un întreg oarecare. Reciproc, dacă vom găsi o anumită soluție formată din numerele neprime între ele p, q, r , atunci punând $p=ax_0, q=ay_0, r=az_0$ (a fiind cel mai mare divizor comun al numerelor p, q și r), substituind ax_0, ay_0, az_0 în ecuație și simplificând cu a^2 , ne vom convinge că x_0, y_0, z_0 reprezintă o soluție formată din numere prime între ele. Așadar, după ce am găsit toate soluțiile prime între ele, vom cunoaște, în general, toate soluțiile ecuației lui Pitagora.

Însă x, y și z fiind numere prime între ele, ele nu pot fi toate trei pare. De asemenea nu pot fi pare nici două dintre ele, deoarece atunci un membru al egalității ar fi divizibil prin 2, iar celălalt nu; dar nici impare nu pot fi toate trei, întrucât suma a două numere impare este pară. Prin urmare, revenind la triunghi, ori sînt impare ambele catete, ori sînt impare una dintre catete și ipotenuza.

Să arătăm că ambele catete nu se pot exprima prin numere impare. În adevăr, dacă una dintre ele se exprimă prin numărul $2q+1$, iar a doua prin numărul $2p+1$ (unde q și p sînt numere întregi), atunci suma pătratelor lor va fi:

$$(2q+1)^2 + (2p+1)^2 = 4q^2 + 4q + 1 + 4p^2 + 4p + 1 = 4(q^2 + q + p^2 + p) + 2.$$

Evident, această sumă este divizibilă prin 2, dar nu și prin 4. Însă pătratul oricărui număr par este divizibil prin 4, iar pătratul oricărui număr impar nu se împarte prin 2. Prin urmare, suma pătratelor a două numere impare nu poate fi nici pătratul unui număr par, nici pătratul unui număr impar, prin urmare nu poate fi pătratul unui număr întreg.

În concluzie, dacă toate cele trei laturi ale triunghiului dreptunghi se exprimă prin numere întregi prime între ele, atunci este posibilă numai următoarea „distribuție” a parității: una dintre

¹⁾ Pitagora nu s-a ocupat de această ecuație, însă ea se leagă de teorema sa și de aici îi provine denumirea.

²⁾ Trei astfel de numere se numesc prime între ele. Vedem că această denumire se aplică nu numai unei perechi de numere, ca la p. 54, ci și mai multor numere întregi.

catete este un număr par, iar cealaltă catetă și ipotenuza sînt numere impare.

Vom nota cu x cateta exprimată prin numărul par și cu y pe cea exprimată prin numărul impar. În acest caz avem dreptul să scriem $x=2v$ și ecuația noastră devine $4v^2 + y^2 = z^2$ sau $4v^2 = z^2 - y^2$; în sfîrșit, aceasta se mai poate scrie astfel:

$$4v^2 = (z+y)(z-y).$$

Suma și diferența a două numere impare sînt totdeauna pare. De aceea, vom pune:

$$z+y=2u, \quad z-y=2t.$$

Se vede ușor că u și t sînt prime între ele și anume unul este par, iar celălalt impar. În adevăr, exprimînd pe z și y prin u și prin t , obținem $z=u+t, y=u-t$. Dacă u și t ar avea un divizor comun, acest divizor ar fi comun și numerelor z și y , ceea ce contrazice ipoteza, conform căreia acestea sînt prime între ele; tot astfel, u și t nu pot avea aceeași paritate, pentru că atunci z , care este egal cu suma lor, ar fi par, ceea ce este imposibil.

Introducînd în ecuația $4v^2 = (z+y)(z-y)$ numerele $2u$ și $2t$ pentru suma și diferența necunoscutelor, vom avea:

$$4v^2 = 4ut \quad \text{sau} \quad v^2 = ut.$$

Aceasta este însă posibil numai în cazul cînd u și t sînt fiecare pătrate, adică dacă $u=a^2, t=b^2$. În adevăr, în produsul ut (egal cu pătratul numărului v) toți factorii primi intră în perechi ¹⁾. Dacă u ar cuprinde un factor nepereche, atunci și t ar trebui să cuprindă un astfel de factor pentru ca să avem o pereche în produsul $ut=v^2$. Aceasta este însă imposibil, deoarece numerele u și t sînt prime între ele și nu au factori comuni. Așadar, în u toți factorii primi trebuie să intre în perechi; același lucru se poate spune și despre t . Prin urmare, u și t sînt pătrate.

Mai observăm că, deoarece numerele $u(=a^2)$ și $t(=b^2)$ sînt prime între ele și au paritatea diferită, înseși numerele a și b vor fi tot prime între ele și de paritate diferită. Prin urmare

$$z=t+u=b^2+a^2,$$

$$y=t-u=b^2-a^2.$$

¹⁾ Ne vom ocupa mai amănunțit de descompunerea în factori primi în cap. XI (p. 121).

Ajungem la următorul rezultat: într-un triunghi dreptunghi, ale cărui laturi sînt egale cu numere întregi prime între ele, ipote-nuza este egală cu suma pătratelor a două numere întregi, prime între ele și de paritate diferită, iar una dintre catete cu diferența pătratelor aceluiași numere. Este valabilă și reciproca: suma și diferența pătratelor a două numere întregi a și b arbitrare dau o soluție a ecuației lui Pitagora, fiindcă în acest caz, a doua catetă este în mod necesar un număr întreg:

$$x^2 = z^2 - y^2 = (b^2 + a^2)^2 - (b^2 - a^2)^2 = \\ = b^4 + 2a^2b^2 + a^4 - b^4 + 2a^2b^2 - a^4 = 4a^2b^2,$$

de unde

$$x = 2ab,$$

adică x este un număr întreg.

Prin urmare, cea mai generală soluție a ecuației lui Pitagora formată din rădăcini prime între ele va fi dată de formulele:

$$x = 2ab,$$

$$y = b^2 - a^2,$$

$$z = b^2 + a^2;$$

toate soluțiile, atît cele formate din rădăcini prime între ele, cît și cele formate din rădăcini neprime între ele, vor fi date de formulele:

$$x = 2abn,$$

$$y = (b^2 - a^2)n,$$

$$z = (a^2 + b^2)n.$$

În aceste relații n este un număr natural cu totul arbitrar, iar a și b sînt numere întregi oarecare, la a căror alegere se impun numai următoarele restricții: 1) b este mai mare decît a ; 2) b și a sînt prime între ele; 3) b și a sînt de paritate diferită.

Vedem că există mai multe posibilități de alegere decît în cazurile considerate pînă acum. Este natural să se întîmple așa, deoarece pînă acum era vorba numai de o singură relație care lega două necunoscute, pe cînd aici relația leagă trei necunoscute. Este limpede că legătura (restricția) a slăbit în ultimul caz.

Să considerăm cîteva soluții numerice ale ecuației lui Pitagora. Dacă $n=1$ (rădăcini prime între ele), obținem următorul șir de soluții:

$a=1$				$a=2$				$a=3$			
b	x	y	z	b	x	y	z	b	x	y	z
2	4	3	5	3	12	5	13	4	24	7	25
4	8	15	17	5	20	21	29	8	48	55	73
6	12	35	37	7	28	45	53	10	60	91	109
8	16	63	65	9	36	77	85	14	84	187	205
10	20	99	101	11	44	117	125	16	96	267	285
...	...	...	...	...	...	...	...	...	...	...	...

Mai departe, putem scrie tabelele pentru $a=4$, $a=5$ etc.

Înmulțind oricare dintre liniile din fiecare tabelă de mai sus cu un număr natural arbitrar, obținem noi șiruri de soluții. De exemplu, înmulțind linia a treia a tabelului a doua cu 2, 3, 4, ... consecutiv, obținem următoarele soluții:

n	x	y	z
1	28	45	53
2	56	90	106
3	84	135	159
4	112	180	212
5	140	225	265
...	...	...	...

Problema nu poate avea alte soluții, în afara celor obținute astfel din tabelele de mai înainte.

După ecuația $x^2 + y^2 = z^2$ este natural să considerăm ecuațiile $x^3 + y^3 = z^3$; $x^4 + y^4 = z^4$ etc. Matematicienii din secolul al XVI-lea și de la începutul secolului al XVII-lea au încercat să rezolve aceste ecuații în numere întregi, însă fără succes.

Abia în a doua jumătate a secolului al XVII-lea, matematicianul francez Fermat, considerînd ecuația generală de forma

$$x^n + y^n = z^n,$$

unde n este un întreg oarecare, a ajuns la concluzia că oricare ar fi $n > 2$, problema este nerezolvabilă în numere întregi.

Pentru $n=1$, $x+y=z$ și orice absolvent al școlii elementare poate rezolva această ecuație; pentru $n=2$ obținem ecuația $x^2+y^2=z^2$, pe care am rezolvat-o mai înainte.

Pierre Fermat (1601—1665), remarcabil jurist și fruntaș al orașului său natal Toulouse, s-a ocupat de matematică în orele libere. Se știe prea puțin despre viața sa; el n-a tipărit cărți. După moartea lui Fermat, fiul său i-a editat manuscrisele. Fermat a întreținut corespondență aproape cu toți marii matematicieni ai epocii. Pascal îl considera cel mai bun matematician al timpului. Concomitent cu Descartes, Fermat a pus bazele geometriei analitice, iar o dată cu Pascal, fundamentele teoriei probabilităților. Cele mai de seamă dintre descoperirile sale se leagă însă de teoria numerelor.

Pe marginea cărții lui Diofant, Fermat a scris următoarele (în limba latină): „Nici cubul în două cuburi, nici pătratul pătratului și, în general, nici o putere în afară de pătrat nu poate fi descompusă în suma a două puteri de același fel; am găsit pentru aceasta o demonstrație uimitoare. Însă lărgimea marginii nu-mi permite să o scriu aici“.

Fermat a lăsat această teoremă nedemonstrată. Nu este singura; Fermat a enunțat multe teoreme interesante, fără a ne lăsa demonstrațiile lor. Adeseori el trimitea intenționat teoreme cunoscuților săi, fără demonstrație, propunându-le astfel să rezolve probleme complicate. Deseori contemporanii săi nu puteau face față acestor probleme, însă în cursul secolelor al XVIII-lea și al XIX-lea ele au fost demonstrate, în afară de două! Una dintre ele (numai una singură din întreaga moștenire bogată a lui Fermat) s-a dovedit greșită¹⁾. O singură dată acest geniu a fost trădat de simțul său matematic. A doua, aceea care a fost scrisă pe marginile cărții lui Diofant, nu a putut fi pînă astăzi nici demonstrată, nici infirmată.

Cei mai buni matematicieni și-au încercat forțele cu ea. Euler a demonstrat că ecuațiile $x^3+y^3=z^3$ și $x^4+y^4=z^4$ nu au soluții în numere întregi, adică a demonstrat teorema lui Fermat pentru $n=3$ și pentru $n=4$ ²⁾. Legendre și Dirichlet au demonstrat-o pentru $n=5$, iar Lamé pentru $n=7$. La jumătatea secolului trecut, Kummer a reușit să demonstreze, cu ajutorul unei teorii dificile

și subtile, că teorema lui Fermat ar putea fi falsă numai pentru anumite valori excepționale ale lui n . Astfel, el a demonstrat că această teoremă este valabilă pentru orice n mai mic de 100¹⁾. Totuși, nici Kummer nu a dat demonstrația completă a valabilității ei.

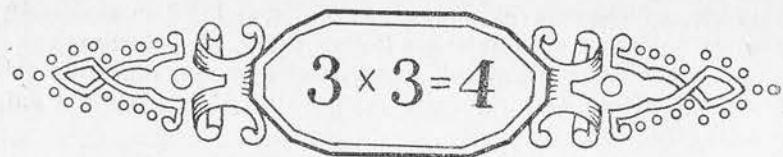
Teorema în sine nu are o importanță principală prea mare. Însă ea a generat o literatură imensă, a dat prilej pentru descoperirea unor noi teorii și metode de rezolvare a unor probleme și a jucat în general un rol atât de important în dezvoltarea matematicii, încît i s-a dat denumirea de marea teoremă a lui Fermat.

¹⁾ În prezent ea este demonstrată pentru orice n mai mic de 619 (precum și pentru anumite valori mai mari).



¹⁾ Ne vom ocupa de ea mai departe, la p. 114.

²⁾ De fapt, demonstrația teoremei pentru $n=4$ a fost dată chiar de Fermat.



CAPITOLUL VIII

O ARITMETICĂ ÎN CARE „TREI ORI TREI FAC PATRU“



În capitolul IV (p. 35) am întâlnit o aritmetică în care $3 \times 3 = 10$. Acest rezultat este valabil în sistemul de numerație cu baza 9. Bineînțeles, atât în acest sistem cât și în oricare altul, numărul trei repetat de trei ori va da nouă; însă în sistemul cu baza nouă numărul nouă, fiind unitatea de ordinul al doilea, se scrie 10. Așa se explică notația paradoxală de mai sus.

Nu vom discuta însă modul de notare. Ceea ce vrem să arătăm este că „trei ori trei fac patru“, conform unui anumit punct de vedere pe deplin rațional și în unele cazuri util. Pentru a înțelege posibilitatea unui astfel de punct de vedere, să revenim la ecuațiile nedeterminate liniare, de care ne-am ocupat în capitolul precedent.

Să considerăm ecuația

$$ax + by = c,$$

unde a, b, c sînt numere întregi, iar a și b sînt prime între ele. În esență, rezolvarea acestei ecuații se reduce la aflarea lui x . Atunci y se determină imediat:

$$y = -\frac{ax - c}{b}.$$

În aceste condiții x trebuie astfel ales, încît expresia lui y să fie un număr întreg. Această expresie va fi cu siguranță întreagă, dacă $ax - c$ este divizibil prin b sau dacă ax împărțit prin b dă restul c . (În adevăr, dacă ax împărțit prin b dă restul c , înseamnă că $ax = bm + c$; scăzînd de aici pe c obținem bm , care este, evident, divizibil prin b).

După ce x a fost determinat, aflarea lui y nu prezintă nici un fel de dificultate; putem chiar să nu-l considerăm de loc pe y . Dar problema aflării lui x poate fi astfel pusă, încît y nici să nu figureze în rezultat. De fapt, aici se cere să se afle x astfel încît produsul ax , împărțit prin b , să dea restul c .

Pentru început, ne ocupăm de cazul cel mai simplu, cînd $a = 1$. Problema devine: să se afle toate numerele x care, împărțite printr-un număr dat b , dau restul c . Acest enunț, simplu în aparență, s-a dovedit deosebit de fecund. El a fost dezvoltat și transformat într-un sistem armonios de către Gauss (1777—1855), care a reușit să facă pe această cale multe descoperiri importante.

Așadar, ne interesează toate numerele care, împărțite printr-un număr determinat, dau un rest anumit. De exemplu, dacă numărul prin care împărțim (el se numește modul¹⁾) este egal cu 7, iar restul cerut este egal cu 2, atunci numerele căutate vor fi:

$$2, 9, 16, 23 \text{ etc.}$$

Ele formează o progresie aritmetică infinită, în care primul termen este 2, iar rația 7.

Numerele care, împărțite prin modul, dau resturi egale se numesc congruente față de acest modul. Prin urmare, numerele 2, 9, 16, 23, ... sînt congruente față de modulul 7. Tot astfel, numerele 1 și 27 sînt congruente față de modulul 13, 103 și 3 față de modulul 10 etc.

Noțiunea de congruență, introdusă de Gauss, are o foarte largă aplicare în matematică; a trebuit să se introducă pentru ea o notație specială (dată tot de Gauss). Dacă a și b , împărțite prin m , dau resturi egale, cu alte cuvinte dacă a și b sînt congruente față de modulul m , scriem:

$$a \equiv b \pmod{m}.$$

Aceasta se citește: „ a este congruent cu b modulo m “. Semnul de congruență ($\equiv$) seamănă cu semnul de egalitate, nu întîmplător ci pentru că proprietățile congruențelor sînt asemănătoare cu proprietățile egalităților.

¹⁾ Cuvîntul „modul“ provine de la latinescul *modulus*, care înseamnă „unitate de măsură“; el se folosește, de obicei, în sens de „divizor“, „împărțitor“. Unele constante care intră la numitorul anumitor formule din fizică și din tehnică se numesc deseori moduli: de exemplu modulul de elasticitate din legea lui Hooke etc.

În afară de congruențele care conțin numere cunoscute, date, cum ar fi $2 \equiv 5 \pmod{3}$, $1000 \equiv 1 \pmod{37}$ etc., mai trebuie considerate congruențe care conțin necunoscute. Atunci sînt posibile trei cazuri: 1) congruența este valabilă pentru orice valori întregi ale literelor pe care le conține; 2) ea este valabilă numai pentru unele; 3) ea nu este valabilă pentru nici un fel de valori ale acestor litere. De exemplu congruența $ax \equiv 2a \pmod{a}$ este valabilă pentru orice x și a întregi (ax și $2a$ dau ambele, împărțite prin a , un rest nul; deci sînt congruente). Dimpotrivă, congruența $2x \equiv 3 \pmod{5}$ valabilă pentru $x=4$ (deoarece $2 \cdot 4 = 8$, împărțit prin 5, dă restul 3) nu este satisfăcută pentru $x=5$, deoarece atunci $2x=10$, iar 10 se împarte fără rest prin modulul 5. În sfîrșit, congruența $2x \equiv 1 \pmod{2}$ nu este verificată pentru nici un x întreg; membrul întîi $2x$ este divizibil prin modul, pe cînd membrul al doilea nu.

A rezolva o congruență înseamnă a afla toate valorile necunoscute care o satisfac (sau a demonstra imposibilitatea ei). Valorile necunoscute care satisfac congruența se numesc soluțiile ei.

Ca și ecuațiile, congruențele pot fi de gradul întîi, al doilea etc., pot conține una, două sau mai multe necunoscute. Iată cîteva exemple de congruențe:

$$2x + 3y \equiv 5 \pmod{21} \text{ (congruență de gradul întîi cu două necunoscute);}$$

$$x^2 + 5x - 3 \equiv 0 \pmod{3} \text{ (congruență de gradul al doilea cu o necunoscută).}$$

Vom studia acum proprietățile cele mai simple ale congruențelor. Să luăm congruența $a \equiv b \pmod{m}$ și să încercăm a o transpune în limbajul obișnuit al egalităților. Aceasta se face destul de ușor. În adevăr, congruența $a \equiv b \pmod{m}$ înseamnă că $a-b$ este divizibil prin m , adică $a-b$ este egal cu produsul lui m cu un număr n . Reciproc: dacă $a-b=mn$, unde n este un întreg, atunci împărțind pe a prin m și pe b prin m , vom obține aceleași resturi. În adevăr, să admitem că numărul a , împărțit prin m , dă restul r_1 , iar b , restul r_2 . Aceasta înseamnă că au loc egalitățile $a=pm+r_1$; $b=qm+r_2$, unde p, q, r_1 și r_2 sînt numere întregi, iar r_1 și r_2 sînt totodată mai mici decît m . Să admitem că $r_1 > r_2$. Scăzînd a doua egalitate din prima, obținem:

$$a-b = (p-q)m + r_1 - r_2$$

sau

$$r_1 - r_2 = (a-b) - (p-q)m = mn - (p-q)m = m(n-p+q).$$

Prin urmare, diferența $r_1 - r_2$ este un multiplu de m . Această diferență este mai mică decît m , deoarece atît descăzutul cît și scăzătorul sînt numere pozitive mai mici decît m ; prin urmare diferența nu poate fi decît nulă, deci $r_1 = r_2$. Însă faptul că a și b , împărțite prin modulul m , dau același rest, se scrie tocmai $a \equiv b \pmod{m}$.

Așadar, egalitatea $a-b=mn$ (sau $a=b+mn$) și congruența $a \equiv b \pmod{m}$ reprezintă exact același lucru. Acolo unde este necesar, putem scrie congruența în locul egalității sau egalitatea în locul congruenței. Ambele exprimă aceeași idee în limbaj diferit.

Congruențele față de același modul pot fi adunate, scăzute și înmulțite (membru cu membru). Să considerăm două congruențe:

$$a \equiv b \pmod{m} \text{ și } c \equiv d \pmod{m}.$$

După cum știm, prima este echivalentă cu egalitatea $a=mn_1+b$, iar a doua cu egalitatea $c=mn_2+d$; adunînd (sau scăzînd) aceste egalități, vom avea $a \pm c = m(n_1 \pm n_2) + b \pm d$. Trecînd din nou la congruențe, vom obține:

$$a \pm c \equiv b \pm d \pmod{m}.$$

Acest rezultat ne arată că avem voie să adunăm (sau să scădem) congruențele membru cu membru.

Înmulțind egalitățile $a=mn_1+b$ și $c=mn_2+d$, obținem:

$$\begin{aligned} ac &= m^2 n_1 n_2 + mn_1 d + mn_2 b + bd = \\ &= m(mn_1 n_2 + n_1 d + n_2 b) + bd. \end{aligned}$$

Dacă vom nota expresia din paranteze (care este evident un număr întreg) cu litera n , vom avea:

$$ac = mn + bd.$$

Aceasta înseamnă că $ac \equiv bd \pmod{m}$; cu alte cuvinte, congruențele cu același modul pot fi înmulțite membru cu membru. Bineînțeles, putem aduna și înmulți nu numai două, ci un număr oarecare de congruențe. De aici obținem imediat următoarea consecință: o congruență care nu conține necunoscute poate fi ridicată la orice putere.¹⁾

Tot atît de simplu se poate demonstra că putem adăuga la ambii membri ai unei congruențe (sau scădea din ei) același

¹⁾ Înmulțirea cu o expresie care conține necunoscute poate să ducă la soluții străine ca în cazul ecuațiilor obișnuite.

număr; de asemenea putem înmulți ambii membri ai unei congruențe cu același număr¹⁾. De exemplu din $a \equiv b \pmod{m}$ rezultă $a+c \equiv b+c \pmod{m}$. În adevăr, să adunăm congruențele:

$$a \equiv b \pmod{m} \text{ și } c \equiv c \pmod{m}$$

(prima este dată, iar a doua este evidentă); obținem:

$$a+c \equiv b+c \pmod{m},$$

ceea ce trebuia demonstrat.

Proprietățile congruențelor ne permit să efectuăm asupra lor aproape toate transformările la care supunem ecuațiile. În particular, putem trece termeni dintr-o parte (mai bine zis, dintr-un membru) a congruenței în cealaltă, schimbând semnele. Împreună cu reducerea termenilor asemenea, aceasta ne permite să dăm tuturor congruențelor forma:

$$(\text{un polinom arbitrar}) \equiv 0 \pmod{m}.$$

De exemplu, congruența

$$x^2 \equiv 1-x \pmod{4}$$

se reduce la:

$$x^2+x-1 \equiv 0 \pmod{4}.$$

La fel congruența

$$3x-y+5 \equiv y+10 \pmod{7}$$

se reduce la congruența:

$$3x-2y-5 \equiv 0 \pmod{7}.$$

În particular, orice congruență de gradul întâi, cu o necunoscută, se poate reduce la următoarea:

$$ax+b \equiv 0 \pmod{m},$$

unde a , b și m sînt numere întregi date (m este pozitiv).

Într-o anumită privință, însă, congruențele sînt „mai neplăcute” decît egalitățile. Ele nu pot fi simplificate totdeauna cu un factor comun. Să studiem mai atent această problemă.

Congruența $22 \equiv 12 \pmod{5}$ este incontestabil adevărată; împărțind prin 5, atît numărul 22 cît și 12, obținem restul 2. Dacă vom împărți ambii membri prin 2, rezultă $11 \equiv 6 \pmod{5}$; și această congruență este adevărată: și 11 și 6 împărțite prin 5

¹⁾ Înmulțirea cu o expresie care conține necunoscute poate să ducă la soluții străine, ca în cazul ecuațiilor obișnuite.

dau restul 1. S-ar părea că totul este în perfectă ordine. Să luăm însă un alt exemplu: $14 \equiv 10 \pmod{4}$. Împărțite prin 4, numerele 14 și 10 dau restul 2. Dacă vom împărți ambii membri prin 2, vom obține $7 \equiv 5 \pmod{4}$, ceea ce este fals, deoarece 7 împărțit prin 4 dă restul 3, iar 5 împărțit prin 4 dă restul 1. Ce se întâmplă aici?

În primul exemplu, ambii membri ai congruenței sînt primi cu modulul. În al doilea, însă, cei doi membri și modulul au un divizor comun, anume 2, iar congruența nu mai poate fi simplificată¹⁾.

Să enunțăm observațiile noastre sub formă de teoreme și să le demonstrăm.

Teorema întâi. *Dacă ambii membri ai unei congruențe au un factor comun și, în afară de aceasta, sînt primi cu modulul, atunci congruența poate fi simplificată cu acest factor.*

Să presupunem că în congruența

$$ad \equiv bd \pmod{m}$$

ambii membri sînt divizibili prin d ; acest număr și modulul sînt prime între ele, adică m și d nu au divizori comuni diferiți de unitate. Congruența noastră poate fi transformată astfel:

$$ad-bd \equiv 0 \pmod{m},$$

adică produsul $d(a-b)$ trebuie să fie divizibil prin m . Prin ipoteză, d și m sînt prime între ele. Prin urmare, trebuie ca $a-b$ să fie divizibil prin m , adică trebuie să aibă loc congruența $a \equiv b \pmod{m}$, ceea ce trebuia demonstrat. Și aici sîntem nevoiți să recurgem la teorema a treia din capitolul VI (p. 50).

Teorema a doua. *Dacă cei doi membri ai unei congruențe și modulul au un factor comun, împărțindu-i prin acest factor se obține o nouă congruență. (Deci, în acest caz, putem simplifica ambii membri ai congruenței, dar totodată și modulul.)*

Să luăm congruența

$$ad \equiv bd \pmod{md},$$

în care ambii membri și modulul se împart prin d . Transpunem ideea exprimată prin congruență în limbajul egalităților:

$$ad = md \cdot n + bd.$$

¹⁾ O întrebare pentru cititor: este posibil oare ca un membru al congruenței să fie prim cu modulul, iar celălalt nu?

Simplificarea acestei egalități cu d ne dă:

$$a = mn + b.$$

Trecînd din nou la congruențe, avem:

$$a \equiv b \pmod{m},$$

ceea ce trebuia demonstrat.

Această teoremă ne explică de ce exemplul al doilea, $14 \equiv 10 \pmod{4}$ a dus, în urma simplificării, la o absurditate. Ambii membri ai congruenței și modulul 4 se împart prin 2. Așadar, nu trebuia să uităm că, la simplificarea prin 2, urma să fie simplificat și modulul, ceea ce ar fi dat $7 \equiv 5 \pmod{2}$.

Deci congruențele sînt „inferioare” egalităților, din punctul de vedere la posibilității de simplificare. În schimb, ele au proprietăți care permit să le supunem unor transformări irealizabile în cazul egalităților. Iată cele mai importante dintre aceste proprietăți: la oricare membru al unei congruențe putem aduna orice număr care este multiplu al modulului; din orice membru al unei congruențe putem scădea orice număr care este multiplu al modulului.

Să le considerăm împreună. Adunăm la ambii membri ai congruenței

$$a \equiv b \pmod{m}$$

(sau să scădem din ei) congruența evidentă $cm \equiv 0 \pmod{m}$; obținem:

$$a + cm \equiv b \pmod{m}.$$

Analog, am putea obține:

$$a \equiv b + cm \pmod{m}.$$

Să vedem ce folos putem trage de pe urma acestei proprietăți. Fie dată congruența:

$$13x \equiv 16 \pmod{7}. \quad (1)$$

Dacă scădem din primul membru $7x$ (acest număr este un multiplu al modulului), obținem:

$$6x \equiv 16 \pmod{7}.$$

Mai departe, scădem din membrul al doilea numărul 14, de asemenea multiplu al modulului. Obținem:

$$6x \equiv 2 \pmod{7}.$$

Simplificînd cu 2 (modulul nu este divizibil prin 2), rezultă congruența foarte simplă:

$$3x \equiv 1 \pmod{7}. \quad (2)$$

Din congruența (1) am obținut congruența (2). Ea este valabilă pentru aceleași valori ale necunoscutei x pentru care era valabilă și congruența inițială (1). Astfel de congruențe se numesc echivalente. Congruența (2) este însă mai simplă decît congruența (1).

Vom studia cîteva probleme a căror rezolvare va ilustra utilizarea congruențelor.

Problema întâi. Care este restul împărțirii prin 9 a numărului $1532^5 - 1$?

Pentru rezolvarea acestei probleme, nu este necesar să efectuăm o înmulțire obositoare și o împărțire plicticoasă. Raționăm astfel:

1530 este divizibil prin 9 (suma cifrelor sale se împarte prin 9). În consecință 1532 dă restul 2 la împărțirea prin 9; aceasta se poate scrie sub forma congruenței:

$$1532 \equiv 2 \pmod{9}.$$

Dar congruențele pot fi înmulțite membru cu membru și, în particular, ambii membri ai congruenței pot fi ridicați la aceeași putere. Să ridicăm congruența noastră la puterea a cincea; vom avea:

$$1532^5 \equiv 32 \pmod{9}.$$

Scădem 27 din membrul al doilea (27 este multiplu al modulului) și obținem:

$$1532^5 \equiv 5 \pmod{9}.$$

Dacă scădem acum cîte o unitate din ambii membri ai congruenței, rezultă:

$$1532^5 - 1 \equiv 4 \pmod{9}.$$

Aceasta înseamnă că $1532^5 - 1$ dă restul 4 la împărțirea prin 9. Problema este rezolvată.

Problema a doua. Care sînt ultimele două cifre ale numărului 99^9 ?

Să vedem mai întâi care sînt ultimele două cifre ale primelor zece puteri ale lui 9. Le găsim ușor:

$$\begin{aligned} 9^1 &= \dots 9 \\ 9^2 &= \dots 81 \\ 9^3 &= \dots 29 \\ 9^4 &= \dots 61 \\ 9^5 &= \dots 49 \\ 9^6 &= \dots 41 \\ 9^7 &= \dots 69 \\ 9^8 &= \dots 21 \\ 9^9 &= \dots 89 \\ 9^{10} &= \dots 01^1) \end{aligned}$$

Ultimul număr, care se termină cu 01, dă restul 1 dacă îl împărțim prin 100, ceea ce se scrie:

$$9^{10} \equiv 1 \pmod{100}.$$

Dacă vom ridica ambii membri ai acestei congruențe la o putere întreagă arbitrară p , vom vedea că orice putere a numărului 9^{10} , adică orice număr de forma 9^{10p} , va fi congruent cu 1, față de modulul 100.

Fie o putere arbitrară a lui nouă, 9^N . Notăm cu p numărul zecilor din N și cu q numărul unităților; cu alte cuvinte, luăm $N = 10p + q$. Am arătat că

$$9^{10p} \equiv 1 \pmod{100}.$$

Înmulțind ambii membri ai acestei congruențe cu 9^q , obținem în primul membru

$$9^{10p} \cdot 9^q = 9^{10p+q} = 9^N,$$

iar în membrul al doilea 9^q , adică

$$9^N \equiv 9^q \pmod{100}.$$

Ultima egalitate ne arată că orice putere N a lui nouă este congruentă, față de modulul 100, cu o putere q a acestuia, dacă exponentul q este egal cu restul împărțirii exponentului inițial

¹⁾ Sînt indicate numai ultimele cifre ale produselor. Celelalte nu ne interesează, așa că nu merită să pierdem timp, calculîndu-le.

prin 10, cu alte cuvinte dacă N și q au ultimele două cifre identice.¹⁾ Așadar, problema noastră se simplifică: ultimele două cifre ale numărului 9^{99} vor fi neapărat aceleași ca și ultimele două cifre ale numărului 9^a , unde a este restul împărțirii prin 10 a exponentului „cu două etaje”, 9^9 . Însă restul împărțirii unui număr prin 10 este egal cu ultima cifră din scrierea zecimală a acestui număr. Pentru numărul 9^9 el este egal cu 9 (v. tabela puterilor lui nouă, dată mai înainte).

Prin urmare, avem:

$$9^{99} \equiv 9^9 \pmod{100},$$

adică 9^{99} și 9^9 au ultimele două cifre identice. Să examinăm din nou tabela cu primele zece puteri ale lui nouă; vedem că 9^9 se termină cu 89; deci 9^{99} se va termina tot cu 89.

Am discutat pînă acum despre transformările congruențelor și despre operațiile cu congruențe. Ar fi normal să trecem la rezolvarea congruențelor de gradul întâi cu o necunoscută; totuși vom proceda altfel. Remarcăm doar că rezolvarea oricărei congruențe poate fi redusă la rezolvarea unei ecuații nedeterminate. Fie de exemplu congruența

$$7x \equiv 3 \pmod{9}.$$

De aici rezultă că diferența $7x - 3$ se împarte prin 9, deci este egală cu produsul dintre 9 și un număr întreg y :

$$7x - 3 = 9y \quad \text{sau} \quad 7x - 9y = 3.$$

Am obținut o ecuație nedeterminată, pe care știm s-o rezolvăm în numere întregi (v. capitolul precedent).

Să cercetăm acum congruențele dintr-un punct de vedere cu totul diferit. Fie dat modulul $m = 5$. Oricare ar fi numerele împărțite prin 5, nu putem obține decît următoarele resturi: 0, 1, 2, 3 și 4. Din acest punct de vedere putem clasifica toate numerele naturale în cinci categorii, după restul pe care îl dau la împărțirea prin 5. Numerele din fiecare categorie formează o progresie

¹⁾ Dacă două numere sînt congruente, adică dau resturi egale față de modulul 100, este evident că, în sistemul zecimal, fiecare dintre ele are la sfîrșit aceleași două cifre.

aritmetică infinită, a cărei rație este egală cu modulul (în exemplul nostru, cu cinci). Iată cele cinci progresii:

$$\begin{aligned} &\div 1, 6, 11, 16, 21, 26, 31, \dots \\ &\div 2, 7, 12, 17, 22, 27, 32, \dots \\ &\div 3, 8, 13, 18, 23, 28, 33, \dots \\ &\div 4, 9, 14, 19, 24, 29, 34, \dots \\ &\div 5, 10, 15, 20, 25, 30, 35, \dots \end{aligned}$$

Evident, fiecare număr se va încadra neapărat în una și numai în una dintre aceste progresii. Progresiile respective se numesc clase față de modulul 5. În mod analog se pot împărți numerele naturale în clase față de orice alt modul.

Toate numerele care fac parte din progresiile considerate (deci absolut toate numerele șirului natural) se numesc resturi¹⁾ față de modulul 5; fiecare rest poate servi ca termen liber în congruența rezolubilă $x \equiv a \pmod{5}$.

Fie congruența de gradul al doilea

$$x^2 \equiv a \pmod{3};$$

ne putem convinge că anumite numere, de exemplu $a=1$, sînt resturi, deoarece congruența $x^2 \equiv 1 \pmod{3}$ are soluții. Alte numere (de exemplu 2) nu sînt resturi: se poate demonstra că $x \equiv 2 \pmod{3}$ nu are soluții. Se spune că 2 nu este un rest pătratic față de modulul 3. Pentru congruențele de gradul întâi, fiecare număr natural este un rest.

Să luăm câte un număr din fiecare clasă:

din prima progresie	6
din a doua progresie	2
din a treia progresie	28
din a patra progresie	14
din a cincea progresie	10

Numerele astfel alese se numesc reprezentanți ai claselor de resturi față de modulul 5; ele formează un sistem complet de resturi față de modulul 5.

Un sistem complet de resturi față de un modul dat se bucură de multe proprietăți remarcabile. Vom considera una dintre ele. În scopul de a o face mai intuitivă, vom recurge la o nouă simplificare: în locul reprezentanților claselor luați la întâmplare, vom lua resturile pozitive cele mai mici corespunzătoare

¹⁾ Cuvîntul „rest” ne amintește că la studiul numerelor întregi considerăm împărțirea ca pe o scădere repetată.

diferitelor clase. În exemplul nostru acestea vor fi numerele 1, 2, 3, 4, 5. Ultimul rest, egal cu modulul, îl înlocuim prin numărul 0, congruent cu el față de acest modul. Obținem următorul sistem de numere:

$$1, 2, 3, 4, 0.$$

Cu numerele unui astfel de sistem efectuăm adunarea, scăderea și înmulțirea conform regulilor obișnuite, însă vom înlocui fiecare rezultat obținut prin cel mai mic rest pozitiv din aceeași clasă. De exemplu, adunînd 3 cu 4 obținem 7; restul cel mai mic al clasei, avînd ca reprezentant numărul 7, este egal cu 2. De aceea vom scrie $3+4=2$. Pentru ca această notație să nu fie supărătoare, vom indica modulul față de care am împărțit în clase toate numerele. Vom scrie $3+4=2 \pmod{5}$. Tot astfel, înmulțind 2 cu 3 obținem 6; acest număr aparține primei clase de resturi față de modulul 5. Față de acest modul, 6 este congruent cu 1. De aceea vom scrie $2 \times 3=1 \pmod{5}$. Pentru a scădea 4 din 3, vom înlocui pe 3 prin reprezentantul imediat mai mare din aceeași clasă, anume 8. Vom obține $8-4=4$, sau, față de modulul 5,

$$3-4=4.$$

Să verificăm; dacă $3-4=4$, atunci $4+4$ (suma diferenței și a scăzătorului) trebuie să fie egală cu 3; în adevăr $4+4=8$, adică un număr congruent cu 3 față de modulul 5.

În aceste condiții, dacă vom efectua operații cu numerele dintr-un sistem de resturi minime, care nu sînt negative, față de un modul oarecare, vom obține întotdeauna numere din același sistem. Mai important este faptul că proprietățile operațiilor obișnuite (adunarea, scăderea și înmulțirea) se păstrează în întregime: comutativitatea și asociativitatea adunării și a înmulțirii, distributivitatea înmulțirii în raport cu adunarea, toate regulile de operații cu parantezele. Mai mult, se constată că fiecare ecuație de gradul întâi cu o necunoscută are o soluție care aparține aceluiași sistem de resturi. Se obține astfel o aritmetică specială, foarte asemănătoare cu cea obișnuită. Deosebirea esențială dintre ele consistă în faptul că prima nu este o aritmetică cu o infinitate de numere, ci numai cu... cinci! În afară de aceasta, aritmetica cu cinci numere nu cunoaște împărțirea.

Se poate confecționa un fel de „sciot” care ilustrează intuitiv această aritmetică. Să tăiem două cercuri din carton, unul mai mare și altul mai mic. În fiecare dintre ele înscriem câte un pentagon regulat: vîrfurile lor le vom nota cu cifrele 1, 2, 3, 4, 0. Suprapunem cercul mic peste cel mare astfel, încît centrele lor

să coincidă și le fixăm cu o piuneză (fig. 5). Vrem să adunăm două numere. Iată cum vom proceda: marcăm primul număr pe cercul mare și aducem în dreptul lui zero de pe cercul mic. Marcăm în gând al doilea număr pe cercul mic. În dreptul

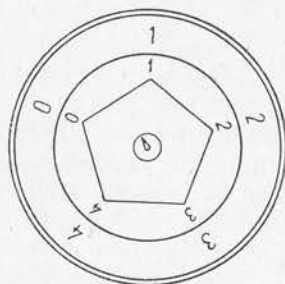


Fig. 5

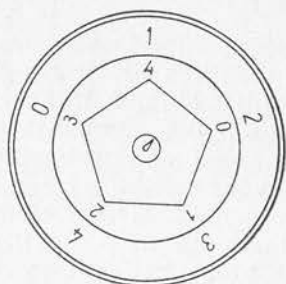


Fig. 6

lui, pe cercul mare, vom găsi suma. De exemplu să adunăm 2 cu 4. În fața lui 2 de pe cercul mare vom aduce zero de pe cercul mic (fig. 6). Lui 4 de pe cercul mic îi corespunde 1 pe cel mare. Prin urmare, avem: $2+4=1 \pmod{5}$.

Cu acest „instrument” putem face și înmulțiri. De exemplu pentru a înmulți 4 cu 3, procedăm astfel: așezăm întâi ambele cercuri în poziția inițială (adică astfel, încât cifrele egale să coincidă). Apoi rotim de trei ori (3 este înmulțitorul) cercul mic cu un unghi egal cu $4/5$ dintr-un cerc (aici numărătorul este egal cu deînmulțitul, iar numitorul cu modulul) și ne uităm în dreptul cărui număr al cercului mare va ajunge zero de pe cercul mic (fig. 7). Vedem că el se va opri în dreptul lui 2. Prin urmare în aritmetica cu cinci cifre $4 \times 3 = 2$.

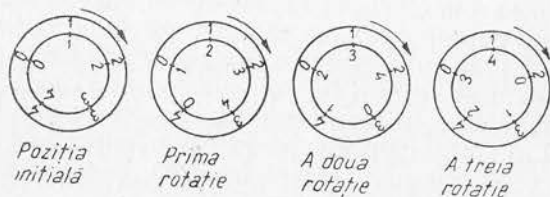


Fig. 7

Folosind acest „sciot” (sau adunarea și înmulțirea obișnuită, urmate de înlocuirea rezultatelor prin resturile minime care corespund față de modulul 5), obținem următoarele table ale adunării și înmulțirii (față de modulul 5):

Tabla adunării

$0+0=0$	$1+0=1$	$2+0=2$	$3+0=3$	$4+0=4$
$0+1=1$	$1+1=2$	$2+1=3$	$3+1=4$	$4+1=0$
$0+2=2$	$1+2=3$	$2+2=4$	$3+2=0$	$4+2=1$
$0+3=3$	$1+3=4$	$2+3=0$	$3+3=1$	$4+3=2$
$0+4=4$	$1+4=0$	$2+4=1$	$3+4=2$	$4+4=3$

Tabla înmulțirii

$0 \times 0 = 0$	$1 \times 0 = 0$	$2 \times 0 = 0$	$3 \times 0 = 0$	$4 \times 0 = 0$
$0 \times 1 = 0$	$1 \times 1 = 1$	$2 \times 1 = 2$	$3 \times 1 = 3$	$4 \times 1 = 4$
$0 \times 2 = 0$	$1 \times 2 = 2$	$2 \times 2 = 4$	$3 \times 2 = 1$	$4 \times 2 = 3$
$0 \times 3 = 0$	$1 \times 3 = 3$	$2 \times 3 = 1$	$3 \times 3 = 4$	$4 \times 3 = 2$
$0 \times 4 = 0$	$1 \times 4 = 4$	$2 \times 4 = 3$	$3 \times 4 = 2$	$4 \times 4 = 1$

Din tabela înmulțirii se vede că $3 \times 3 = 4$. Am ajuns deci la aritmetica pe care am promis-o în titlul capitoului.

În exemplele menționate am operat cu sisteme de numere în care sînt stabilite numai trei operații: adunarea, scăderea și înmulțirea. În matematică astfel de sisteme de numere se numesc inele. Mulțimea tuturor numerelor întregi (pozitive și negative, împreună cu zero) formează și ele un inel, însă acest inel are o infinitate de elemente. De asemenea, formează un inel mulțimea tuturor polinoamelor cu coeficienți întregi, de toate gradele posibile în raport cu litera x . Suma, diferența și produsul unor polinoame de acest fel vor fi, la rîndul lor, polinoame asemănătoare; dimpotrivă, împărțirea duce aproape în toate cazurile la fracții algebrice. Mulțimea numerelor naturale nu este un inel, deoarece diferența a două numere naturale poate să nu fie un număr natural; de exemplu $5-8=-3$, iar „minus trei” este un număr întreg, însă nu natural.

În afară de sistemele de numere în care sînt definite trei operații, putem considera și sisteme în care sînt verificate toate cele patru operații, rezultatul fiind întotdeauna un număr din sistemele respective. Dintre acestea face parte mulțimea tuturor numerelor raționale (adică întregi și fracționare): suma, diferența, produsul și cîțul lor sînt tot numere raționale. Astfel de sisteme de numere se numesc corpuri. Toate numerele raționale formează un corp. Toate numerele reale (cele raționale împreună cu cele iraționale) formează de asemenea un corp; numerele complexe formează și ele un corp. În studiul corpurilor, la fel ca și în aritmetica obișnuită, împărțirea prin zero este „strict interzisă”.

În afară de inele și corpuri se consideră uneori și sisteme de numere în care sînt realizabile numai două operații: adunarea și scăderea. Înmulțirea și împărțirea pot da numere neapartinind sistemului. Astfel de sisteme se numesc grupuri.

Vorbind despre inele, am amintit în treacăt „inelul polinoamelor”. Nu are sens să vorbim despre un asemenea inel, deoarece inelul se referă la o anumită mulțime de numere, iar polinoamele nu sînt numere. Putem însă extinde noțiunile de grup, inel și corp, considerînd nu numai sisteme de numere, ci și sisteme de obiecte, semne, mărimi arbitrare cu care efectuăm anumite operații. Studiul grupurilor, inelelor și corpurilor de diferite genuri, adică al sistemelor cu două, trei sau patru operații, indiferent de obiectele din care sînt constituite, face obiectul algebrei superioare. Aritmetica se ocupă în primul rînd de proprietățile numerelor. Această trăsătură apare deosebit de clară în teoria numerelor prime, de care ne vom ocupa în capitolele următoare.



CAPITOLUL IX

DIVIZIBIL SAU NU ?



ă lăsăm corpurile și inelele, și să revenim la probleme aparținînd aritmeticii. Vom cerceta criteriile de divizibilitate. Criteriile de divizibilitate prin 2, 3, 4, 5, 6, 8, 9, 10, 25 sînt unanim cunoscute. Facem doar observația că, în diferitele sisteme de numerație, criteriile de divizibilitate au forme diferite. De exemplu criteriul de divizibilitate prin 2, în sistemul zecimal, se enunță astfel: „Se împart prin 2 toate numerele care au ultima cifră pară”. Să presupunem că folosim sistemul de numerație cu baza trei. În acesta numărul zece se scrie **101**, adică se termină cu o cifră impară; totuși, aici ca și în oricare alt sistem, numărul zece este divizibil prin 2, pentru că divizibilitatea prin 2 este o proprietate intrinsecă a numărului 10, cu totul independentă de sistemul în care îl scriem. Prin urmare, un criteriu de divizibilitate valabil în sistemul zecimal ar putea fi greșit într-un alt sistem. Desigur, există și propoziții referitoare la divizibilitate, valabile în orice sistem de numerație, cum ar fi, de exemplu, următoarea: „diferența dintre cubul unui număr impar și numărul însuși este divizibilă prin 6”. De aceste propoziții ne vom ocupa în capitolul următor.

Să ne oprim întîi asupra regulii de divizibilitate prin 9, care este bine cunoscută. Aceasta ne va ajuta să înțelegem mai bine metodele care se folosesc la deducerea diferitelor criterii de divizibilitate.

Criteriul de divizibilitate prin 9 se bazează pe faptul că orice număr format din unu urmat de zerouri (adică orice putere a lui

zece), în sistemul zecimal, dă restul 1 cînd îl împărțim prin 9. În adevăr,

$$\underbrace{100 \dots 00}_{n \text{ zerouri}} = 10^n = \underbrace{99 \dots 9}_{n \text{ cifre } 9} + 1.$$

Primul termen, format în întregime din cifre 9, este divizibil prin 9. De aceea, restul împărțirii lui 10^n prin 9 va fi în mod necesar 1.

Mai departe să considerăm un număr arbitrar, de exemplu 4351. Împărțindu-l prin 9, fiecare mie dă ca rest 1. Așadar, patru mii vor da restul 4. Tot astfel, trei sute împărțite prin 9 vor da restul 3, cinci zeci restul cinci; mai rămîne unu (numărul de unități din 4351). Ca rezultat se obține:

$$4351 = (\text{un număr divizibil prin 9}) + 4 + 3 + 5 + 1.$$

Dacă suma de resturi $4+3+5+1$ (care reprezintă tocmai „suma cifrelor” ce compun numărul dat) este divizibilă prin 9, atunci numărul se împarte prin 9. De aici urmează concluzia: dacă „suma cifrelor” unui număr dat este divizibilă prin 9, și numărul însuși va fi divizibil prin 9.

Am scris între ghilimele cuvintele „suma cifrelor” pentru că, riguros vorbind, nu avem voie să adunăm cifrele, deoarece cifra este un simbol pentru scrierea unui număr. Se adună numerele reprezentate de diferitele cifre ale numărului considerat; pentru a scurta exprimarea s-a convenit însă să se spună „suma cifrelor”.

Să reluăm raționamentul, folosind noțiunea de congruență. Împărțind numărul 10 prin 9 rezultă restul 1, adică 10 și 1 sînt congruente față de modulul 9:

$$10 \equiv 1 \pmod{9}.$$

Să ridicăm la o putere arbitrară m ambii membri ai congruenței; obținem:

$$10^m \equiv 1^m \pmod{9}.$$

Înmulțim apoi ambii membri ai acestei congruențe cu un număr arbitrar N ; avem:

$$N \cdot 10^m \equiv N \pmod{9}.$$

Rezultatul obținut poate fi enunțat astfel: produsul dintre un număr arbitrar N și o putere a lui 10 dă, la împărțirea prin 9, același rest ca și împărțirea numărului N prin 9.

Să considerăm acum un număr format din cifrele $a, b, \dots, k, l$; îl scriem:

$$ab \dots kl,$$

avînd grijă să menționăm că nu este produsul numerelor $a, b, \dots$, ci numărul care conține l unități, k zeci etc. El mai poate fi pus sub forma:

$$a \cdot 10^n + b \cdot 10^{n-1} + \dots + k \cdot 10 + l.$$

Aranjăm în formă de coloană șirul de congruențe:

$$\left. \begin{array}{l} a \cdot 10^n \equiv a \\ b \cdot 10^{n-1} \equiv b \\ \cdot \cdot \cdot \cdot \cdot \\ k \cdot 10 \equiv k \\ l \equiv l \end{array} \right\} \pmod{9}.$$

Să adunăm membru cu membru aceste congruențe. În membrul întîi vom avea

$$a \cdot 10^n + b \cdot 10^{n-1} + \dots + k \cdot 10 + l,$$

adică tocmai numărul dat, iar în membrul al doilea vom obține suma cifrelor sale. Prin urmare, orice număr și suma cifrelor sale sînt congruente față de modulul 9, ceea ce înseamnă că ori sînt ambele divizibile prin 9, ori nu.

Criteriul de divizibilitate prin 9 se folosește și în următorul joc instructiv. Propuneți unei persoane să scrie, fără să vă arate, orice număr de 3 sau 4 cifre distincte. Cereți-i să permute cifrele în orice ordine vrea; el va obține atunci un nou număr. Spuneți apoi persoanei să scadă numărul mai mic din cel mai mare și să taie o cifră a diferenței obținute. În sfîrșit, să vă comunice suma celorlalte cifre. Imediat veți putea să-i spuneți care era cifra tăiată.

În adevăr, atît numărul inițial, cît și cel obținut prin permutare, au aceeași sumă a cifrelor; cu alte cuvinte, la împărțirea prin 9 ele dau același rest, deci diferența lor este divizibilă prin 9. Dacă însă această diferență este divizibilă prin 9, înseamnă că și suma cifrelor ei se împarte prin 9. Vi s-a spus suma tuturor cifrelor, cu excepția uneia. Prin urmare, cifra tăiată trebuie să completeze suma indicată de partener, pînă la cel mai apropiat multiplu al lui 9. De exemplu dacă numărul scris era 2365, iar după permutare s-a obținut 3652, diferența lor va fi 1287. Această diferență, deci și suma cifrelor ei $1+2+8+7=18$, este divizibilă prin 9. Dacă se taie cifra 2, rămîn cifrele a căror

sumă este $1+8+7=16$. Când partenerul vă spune că a obținut 16, completați acest număr pînă la cel mai apropiat multiplu de 9 mai mare decît acest număr, adică pînă la 18 (multiplii lui 9 sînt: $1\cdot 9=9$, $2\cdot 9=18$, $3\cdot 9=27$, ...; cel mai apropiat de 16 și mai mare decît el va fi 18). Evident, găsiți $18-16=2$, adică tocmai cifra tăiată. Dacă suma cifrelor netăiate este ea însăși multiplu de 9, este evident că și cifra tăiată trebuie să fie multiplu de 9, adică să fie ori 9 ori 0. În acest caz veți fi nevoiți să spuneți: „a fost tăiat ori un 9, ori un 0“.

Vom cerceta acum criteriul de divizibilitate prin 11. El se bazează pe aceleași considerente ca și criteriul de divizibilitate prin 9. După cum 10, 100, 1000 etc. (o unitate urmată de orice număr de zerouri) împărțite prin 9 dau restul 1, tot astfel 100, 10000, 1000000 (în general o unitate urmată de un număr par de zerouri) dau restul 1 la împărțirea prin 11¹⁾. Cu alte cuvinte,

$$100^n \equiv 1 \pmod{11}.$$

Să considerăm un număr arbitrar, de exemplu 57385. Il împărțim în grupe de câte două cifre, de la dreapta spre stînga, cum procedăm la extragerea rădăcinii pătrate. În acest caz, în ultima grupă din stînga s-ar putea să rămînă o singură cifră (cum se întîmplă în exemplul nostru: 5 73 85). Ce reprezintă prima grupă? Cinci zeci de mii: $5 \times 10\,000$. Fiecare zece mii dă restul 1 la împărțirea prin 11, adică cinci zeci de mii vor da la împărțirea prin 11 restul 5. Grupul următor reprezintă 73 de sute. Fiecare sută, împărțită prin 11, dă restul 1. Prin urmare, 73 de sute vor da restul 73. Mai rămîne ultima grupă din dreapta: 85. Așadar, numărul nostru va avea forma:

$$57385 = (\text{un număr divizibil prin } 11) + 5 + 73 + 85,$$

adică este compus dintr-un număr divizibil prin 11 plus „suma grupelor“.

De aici obținem următoarea regulă: dacă „suma grupelor“ este divizibilă prin 11, va fi divizibil prin 11 și numărul însuși.

În exemplul nostru, suma grupelor este $5+73+85=163$. Rezultatul obținut nu se împarte prin 11; deci nici numărul 57385 nu se împarte prin 11. Dacă la adunarea grupelor vom obține un număr mare, acesta poate fi la rîndul său descompus în grupe; cercetăm suma acestor ultime grupe. În exemplul nostru avem $163=163$. Adunînd grupele $1+63=64$, obținem un număr nedivizibil prin 11; deci nici numărul inițial nu va fi divizibil.

¹⁾ Propunem cititorului să demonstreze aceasta.

Alt exemplu: 563035 este divizibil prin 11. În adevăr, împărțirea în grupe dă 56 30 35 (aici prima grupă din stînga are două cifre). Adunăm grupele $56+30+35=121$. Suma grupelor se împarte prin 11, deci și 563035 va fi divizibil prin 11.

Nu trebuie să ne închipuim că există numai cîte un singur criteriu de divizibilitate pentru fiecare număr. Iată încă un criteriu de divizibilitate prin 11. Să adunăm separat toate cifrele numărului dat care ocupă poziții pare și toate cele care ocupă poziții impare, scăzînd apoi din suma mai mare pe cea mai mică¹⁾. Dacă diferența este divizibilă prin 11 (sau este egală cu zero dat fiind că zero se împarte prin orice număr), atunci și numărul dat respectiv va fi divizibil prin 11.

Să luăm un exemplu. Fie numărul 8230541. Pozițiile impare (socotind de la dreapta) sînt ocupate de cifrele 1, 5, 3, 8; adunînd aceste cifre, obținem $1+5+3+8=17$. În pozițiile pare avem cifrele 4, 0, 2; suma lor este $4+0+2=6$. Diferența $17-6=11$ se împarte prin 11. Deci și numărul 8230541 este divizibil prin 11.

Propunem cititorului să se gîndească singur cum se poate demonstra acest criteriu de divizibilitate. Raționamentul va fi deosebit de simplu dacă va folosi noțiunea de congruență.

În legătură cu criteriile de divizibilitate prin 11, vom studia următoarea problemă.

Problemă. Să se scrie cel mai mic multiplu de 11 compus din șase cifre, prima cifră fiind 7 și toate celelalte distincte.

Să scriem după 7 patru cifre, începînd cu un zero, în ordine crescătoare: 70123. În felul acesta am obținut cel mai mic număr din categoria căutată. Mai rămîne să adăugăm ultima cifră pentru ca întregul număr să fie divizibil prin 11.

Suma cifrelor din pozițiile impare (socotim de la stînga) este $7+1+3=11$; suma cifrelor din pozițiile pare este 2. Pentru ca diferența acestor sume să fie divizibilă prin 11 sau egală cu 0, ultima cifră trebuie să fie nouă ($7+1+3=0+2+9$). Așadar, numărul căutat este 701239.

Cu totul analog este și criteriul de divizibilitate prin 37. Numărul 1000 și toate puterile sale (adică numerele formate dintr-o unitate urmată de un număr de zerouri multiplu

¹⁾ Bineînțeles, în acest caz este indiferent dacă socotim cifrele de la dreapta la stînga sau de la stînga la dreapta; dacă numărul de cifre este impar, atunci fiecare cifră va avea aceeași paritate atît din stînga cît și din dreapta; dacă numărul de cifre este par, atunci luîndu-le de la stînga sau de la dreapta, paritatea cifrelor se va schimba, însă suma cifrelor pare va rămîne egală cu suma cifrelor impare sau va fi diferită de ea.

de 3) dau, la împărțirea prin 37, un rest egal cu 1. În adevăr, 999 este divizibil prin 37 ($999:37=27$). Așadar, avem:

$$1000 \equiv 1 \pmod{37} \text{ și } 1000^n = 10^{3n} \equiv 1 \pmod{37}.$$

Cînd încercăm să stabilim dacă un număr se divide prin 37, trebuie să împărțim acest număr în grupe de cîte trei cifre, de la dreapta spre stînga. În aceste condiții, ultima grupă din stînga poate să conțină o cifră, două sau trei. Dacă suma grupelor este divizibilă prin 37, tot numărul va fi divizibil prin 37. De exemplu 25 012 este divizibil prin 37. Împărțindu-l pe grupe, căpătăm 25 012; suma grupelor este $25+12=37$.

Criteriile de divizibilitate prin 7 și prin 13 se bazează pe faptul că 1001 se împarte prin 7 și prin 13. De altfel, 1001 este divizibil și prin 11, astfel că, în treacăt, vom obține și al treilea criteriu de divizibilitate prin 11.

Să luăm un număr, de exemplu 357 285. Acest număr conține 357 de mii și 285 de unități simple. El se poate scrie astfel: $357\,000 + 285$. Să adunăm și să scădem 357; în urma acestei operații nu se va schimba nimic. Efectuăm apoi transformările simple: $357\,285 = 357\,000 + 285 + 357 - 357 = 357(1\,000 + 1) + 285 - 357 = 357 \cdot 1\,001 - (357 - 285)$.

Primul termen este evident divizibil prin 1001. Rămîne deci să vedem dacă expresia din paranteză (diferența dintre numărul de mii al numărului nostru și numărul de unități simple)¹⁾ este divizibilă prin 7, prin 11 sau prin 13. Dacă această diferență este divizibilă, atunci este divizibil și numărul însuși. Menționăm că numărul de mii poate fi mai mic decît numărul unităților simple; bineînțeles, atunci vom scădea numărul mai mic din cel mai mare.

Să considerăm un alt număr: 208 824 525. El cuprinde 208 824 mii și 525 unități simple. Să scădem din numărul miilor numărul unităților $208\,824 - 525 = 208\,299$. Trebuie să aflăm dacă acest număr se împarte prin 7, prin 11 sau prin 13. Repetăm procedeul de mai înainte. Numărul de unități (299) este acum mai mare decît numărul de mii (208). Scădem numărul mai mic din cel mai mare: $299 - 208 = 91$. Numărul obținut 91 se împarte prin 7 și prin 13, însă nu și prin 11. Așadar, 208 824 525 va fi divizibil prin 7 și prin 13, dar nu va fi divizibil prin 11.

¹⁾ Nu este vorba despre ordine, ci despre clasa miilor și despre clasa unităților simple.

În legătură cu proprietățile numărului 1001 există un interesant joc distractiv. Propuneți cuiva să scrie orice număr de trei cifre, fără să-l vedeți. Cereți persoanei în cauză să adauge, în dreapta numărului scris, numărul însuși (de exemplu dacă scriese inițial 167, va avea acum 167 167). Cereți-i să împartă rezultatul prin 7. Împărțirea va decurge în bune condiții, deși, la prima vedere, un număr luat la întîmplare nu trebuie neapărat să se împartă prin 7. Propuneți partenerului să împartă rezultatul prin 11; iarăși operația va fi încununată de succes. În sfîrșit, spuneți-i să împartă ultimul rezultat prin 13; împărțirea se va face iarăși fără rest, iar rezultatul va fi numărul scris inițial.

„Secretul” jocului este cît se poate de simplu. Repetind în dreapta numărul pe care l-am scris nu înseamnă nimic altceva decît înmulțirea numărului inițial cu 1001 (de exemplu, dacă am scris 167 vom avea $167\,167 = 167\,000 + 167 = 167(1\,000 + 1) = 167 \cdot 1\,001$). Însă $1001 = 7 \cdot 11 \cdot 13$. Prin urmare, împărțind pe 167 167 consecutiv prin 7, 11 și 13, l-am împărțit prin 1001. Inițial, am înmulțit numărul cu 1001, iar apoi l-am împărțit prin același număr. Este evident că toate împărțirile s-au desfășurat în bune condiții și că rezultatul este tocmai numărul inițial.

Criteriile de divizibilitate pentru același număr diferă de la un sistem de numerație la altul. Astfel, în sistemul de numerație cu baza 3, un număr care se termină printr-o cifră impară, poate fi divizibil prin 2. Să stabilim criteriul de divizibilitate prin 2, în sistemul de numerație ternar. La împărțirea prin 2, numărul 3 dă restul 1. Același lucru se poate spune despre orice putere a lui 3, deoarece fiecare putere a lui 3, neconținînd un factor egal cu 2, va da restul 1 la împărțirea prin 2. Reluînd raționamentele pe care le-am folosit la deducerea criteriului de divizibilitate obișnuit pentru 9, ne convingem că în sistemul ternar se împart prin 2 numerele care au suma cifrelor divizibilă prin 2 și numai aceste numere. De exemplu numărul 10 201¹⁾, a cărui sumă a cifrelor este egală cu 4, trebuie să fie divizibil prin 2. În adevăr, numărul 10 201 este egal cu $1 \cdot 3^4 + 0 \cdot 3^3 + 2 \cdot 3^2 + 0 \cdot 3 + 1 = 81 + 18 + 1 = 100$; evident 100 este divizibil prin 2.

Vom cerceta acum problema generală: *să se afle toate sistemele de numerație în care criteriul de divizibilitate al unui număr arbitrar printr-un număr dat a este divizibilitatea sumei cifrelor sale prin numărul a.*

¹⁾ Ca și în capitolele IV și V, caracterele grase reprezintă numere scrise într-un sistem nezeecimal, în cazul de față în sistemul ternar.

În primul rând, observăm că acest criteriu de divizibilitate poate fi enunțat și astfel: diferența dintre orice număr și suma cifrelor sale trebuie să fie divizibilă prin a . În acest caz (și numai în acest caz) din divizibilitatea prin a a oricărui număr va rezulta divizibilitatea prin a a sumei cifrelor sale și reciproc.

Să notăm cu n baza sistemului de numerație căutat. Ca bază a sistemului de numerație, numărul n se va scrie: 10 ; suma cifrelor sale este egală cu unitatea. Așadar, diferența dintre număr și suma cifrelor sale, $n-1$, trebuie să fie divizibilă prin a , ceea ce se scrie $n-1=ma$, unde m este un număr natural arbitrar (sau zero). De aici rezultă că baza n a sistemului de numerație trebuie să fie egală cu un multiplu al numărului a , la care se adună 1:

$$n=ma+1.$$

Reciproc: din această egalitate rezultă că orice putere a lui n va da la împărțirea prin a restul 1. În adevăr, egalitatea noastră exprimă exact același lucru ca și congruența

$$n \equiv 1 \pmod{a};$$

ridicînd la o putere k această congruență, obținem:

$$n^k \equiv 1 \pmod{a}.$$

Dacă însă orice putere a bazei sistemului de numerație dă restul 1 la împărțirea prin a , atunci repetînd cuvînt cu cuvînt deducerea criteriului obișnuit pentru 3 sau pentru 9, ne convingem că divizibilitatea prin a a sumei cifrelor unui număr garantează divizibilitatea prin a a numărului însuși.

Așadar, criteriul de divizibilitate va fi adevărat în toate sistemele de numerație a căror bază este cu o unitate mai mare decît un multiplu arbitrar al lui a . De exemplu divizibilitatea sumei cifrelor va garanta împărțirea unui număr prin 9, nu numai în sistemul zecimal ($10=1\cdot 9+1$), ci și în sistemul cu baza 19 ($19=2\cdot 9+1$) și în cel cu baza 28 ($28=3\cdot 9+1$) și în toate sistemele a căror bază este de forma $9m+1$. Dar acest criteriu de divizibilitate nu va avea loc în nici un alt sistem de numerație.

Problemă. Să se afle sistemul cu cea mai mică bază în care au loc următoarele criterii de divizibilitate:

1° dacă suma cifrelor unui număr este divizibilă prin 5, atunci și numărul se împarte prin 5;

2° dacă numărul format din ultimele două cifre ale unui număr arbitrar se împarte prin 7, atunci și numărul inițial este divizibil prin 7.

Din problema precedentă știm că prima condiție poate fi satisfăcută luînd ca bază a sistemului de numerație un număr de forma $5m+1$:

$$n=5m+1.$$

Să trecem la a doua condiție. Dacă divizibilitatea unui număr prin 7 este determinată de divizibilitatea prin 7 a numărului format de ultimele sale două cifre, înseamnă că unitatea de ordinul al treilea $100=n^2$ trebuie să se împartă prin 7¹). Atunci orice număr de unități de ordinul al treilea se va împărți prin 7 și problema se reduce la cercetarea primelor două ordine. Așadar, n^2 trebuie să fie divizibil prin șapte: $n^2=7p$. Pentru ca membrul al doilea al acestei egalități să fie un pătrat perfect, numărul p trebuie să fie egal cu 7 înmulțit cu un pătrat perfect: $p=7k^2$; vom avea deci $n^2=49k^2$ sau $n=7k$.

Pentru determinarea lui n , am obținut două ecuații liniare cu trei necunoscute

$$n=7k \text{ și } n=5m+1.$$

Egalînd membrii din dreapta, obținem o ecuație nedeterminată liniară cu două necunoscute

$$7k=5m+1 \text{ sau } 7k-5m=1.$$

Știm să rezolvăm astfel de ecuații în numere întregi. Găsim ușor:

$$m=4+5t, \quad k=3+7t,$$

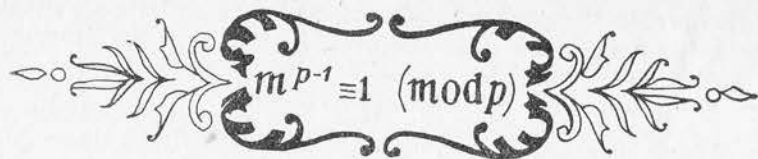
unde t este un întreg arbitrar. Prin urmare, $n=21+49t$. Valoarea pozitivă minimă $n=21$ se obține pentru $t=0$.

Deci cea mai mică bază a unui sistem de numerație în care au loc criteriile de divizibilitate enunțate este 21.

După ce am analizat problema legăturii dintre criteriile de divizibilitate și diferitele sisteme de numerație, vom trece la teoreme despre divizibilitatea numerelor, care nu depind de sistemul de numerație.

¹⁾ Astfel, în sistemul zecimal, criteriul de divizibilitate prin 4 sau 25 se bazează pe divizibilitatea unității de ordinul al treilea (suta) prin aceste numere.





CAPITOLUL X

IARĂȘI DESPRE DIVIZIBILITATE. O TEOREMĂ „MARE”, CUNOSCUTĂ SUB NUMELE DE „MICA TEOREMĂ”



cupîndu-ne de problema triunghiurilor lui Pitagora (p. 75), am fost nevoit să recurgem la propoziții ca: „suma sau diferența a două numere pare sau impare reprezintă numere pare”. Aceste propoziții aparțin incontestabil teoriei divizibilității; însă spre deosebire de criteriile de divizibilitate, considerate în capitolul precedent și legate în mod esențial de alegerea sistemului de numerație, aici alegerea sistemului de numerație nu joacă nici un rol.

Ca prim exemplu să studiem diferența dintre pătratul unui număr impar și unitate, adică expresia m^2-1 , unde m este un număr impar. Ne putem convinge ușor că, oricare ar fi m (impar), această diferență trebuie să fie divizibilă prin 8. În adevăr, ea se descompune în factori:

$$m^2-1=(m-1)(m+1).$$

Pentru că m este un număr impar, ambii factori din membrul al doilea vor fi pari, mai mult, vor fi numere pare vecine, deoarece diferența lor este $m+1-(m-1)=2$. Însă dintre două numere pare vecine, unul este în mod necesar divizibil prin 4¹⁾. Așadar, unul dintre factori este divizibil prin 4, iar al doilea conține factorul 2. Deci întregul produs va fi divizibil prin $2 \cdot 4=8$.

¹⁾ În adevăr, dacă unul dintre numere nu se împarte prin 4, cu toate că este par, atunci la împărțirea prin 4 el poate da numai restul 2, adică să fie de forma $4n+2$. Însă vecinii pari ai acestui număr vor fi $(4n+2) \pm 2$, adică $4n$ și $4n+4$, ultimele două numere fiind ambele multipli de 4.

Putem raționa și astfel: din moment ce n este impar, prin ipoteză, înseamnă că îl putem scrie sub forma $2k+1$, unde k este un număr arbitrar (natural sau zero). Obținem:

$$m^2-1=(2k+1)^2-1=4k^2+4k+1-1=4k(k+1).$$

Unul dintre cele două numere vecine k și $k+1$ este în mod necesar par. Deci, în expresia noastră va intra, pe lângă coeficientul 4, încă un factor egal cu 2; prin urmare vom avea aici un factor egal cu $4 \cdot 2=8$, adică tocmai ceea ce trebuia să demonstrăm.

Dînd numărului m valorile 1, 3, 5, 7, 9, ... obținem următoarele numere multipli de 8:

m	1	3	5	7	9 ...
m^2-1	0	8	24	48	80 ...

Să considerăm acum diferența dintre cubul unui număr arbitrar și acest număr. După cum se arată ușor, această diferență este divizibilă prin 6. În adevăr, să luăm un număr arbitrar m ; diferența dintre cubul acestui număr și numărul însuși este egală cu m^3-m . Descompunînd în factori, această expresie rezultă:

$$m^3-m=m(m-1)(m+1)=(m-1)m(m+1).$$

Cu alte cuvinte, diferența dintre cubul unui număr natural și numărul însuși este întotdeauna produsul a trei numere naturale consecutive. Din trei numere naturale consecutive, cel puțin unul este divizibil prin 2 și altul prin 3¹⁾.

Prin urmare, diferența dintre cubul unui număr natural și numărul însuși este divizibilă prin $2 \cdot 3=6$, ceea ce voiam să demonstrăm.

Al treilea exemplu îl constituie o problemă propusă la olimpiade și concursuri școlare. Iată enunțul acestei probleme: *să se demonstreze că, pentru orice număr natural m , expresia m^5-5m^3+4m este divizibilă prin 120.*

Pentru $m=1$ și $m=2$, demonstrația este imediată, deoarece pentru aceste valori trinomul respectiv este egal cu zero, iar zero

¹⁾ În adevăr, să considerăm trei numere consecutive: $k, k+1, k+2$. Primul are ori forma $k=3n$, ori $k=3n+1$, ori $k=3n+2$, deoarece la împărțirea prin 3 nu sînt posibile decît resturile 0, 1, 2. În cazul $k=3n$, problema este clară. Dacă însă $k=3n+1$, atunci $k+2=3n+3$ și este divizibil prin 3. În sfîrșit, cînd $k=3n+2$, rezultă $k+1=3n+3$, care este de asemenea divizibil prin 3. În toate cazurile posibile, unul dintre cele trei numere consecutive este multiplu de 3.

se consideră multiplu al oricărui număr, deci și a lui 120. De aceea vom considera cazurile când $m > 2$.

Efectuăm următoarele transformări evidente:

$$\begin{aligned} m^5 - 5m^3 + 4m &= m(m^4 - 5m^2 + 4) = m(m^4 - 4m^2 - m^2 + 4) = \\ &= m[(m^4 - 4m^2) - (m^2 - 4)] = m[m^2(m^2 - 4) - (m^2 - 4)] = \\ &= m(m^2 - 4)(m^2 - 1) = (m - 2)(m - 1)m(m + 1)(m + 2). \end{aligned}$$

Oricare ar fi m , trinomul se descompune în cinci factori; pentru $m > 2$, acești factori sînt cinci numere naturale consecutive. În succesiunea celor cinci numere naturale vor exista cel puțin două numere pare vecine; deci trinomul va fi divizibil prin 8. Mai departe, în șirul celor cinci numere există cel puțin un număr divizibil prin 3 (după cum am văzut, chiar primii trei factori garantează divizibilitatea prin 3). În sfîrșit, considerații analoge cu cele din nota de picior de la p. 107, ne conduc la concluzia că produsul celor cinci numere naturale consecutive trebuie să fie divizibil prin 5. Așadar, trinomul inițial este divizibil prin numerele 8, 3 și 5, care sînt prime între ele; prin urmare, el se va împărți și prin produsul lor, adică prin 120.

În tabela următoare sînt date cîteva valori ale trinomului, corespunzătoare unor valori diferite ale numărului m :

m	1	2	3	4	5	...
$m^5 - 5m^3 + 4m$	0	0	120	720	2 520	...

Cele trei exemple menționate sînt foarte instructive, cu tot caracterul lor întrucîtva artificial. Ele ne conduc spre două teoreme interesante. În primul rînd am constatat că diferența $m^3 - m$ este divizibilă prin 3. Tot astfel putem demonstra că $m^5 - m$ este divizibil prin 5, deși demonstrația este mai grea. Imediat rezultă că $m^2 - m$ este divizibil prin 2. S-ar putea însă ca $m^4 - m$ să nu fie divizibil prin 4, pentru unele valori ale lui m . Astfel cînd $m = 2$, avem $m^4 - m = 16 - 2 = 14$, adică un număr nedivizibil prin 4. Se pune întrebarea: pentru ce valori a lui a , diferența $m^a - m$ este divizibilă prin exponentul a , oricare ar fi m ? Această problemă a fost rezolvată de Fermat. Ne vom ocupa de ea la sfîrșitul capitolului de față.

În ceea ce privește a doua teoremă la care duc exemplele noastre, putem spune următoarele: am văzut că produsul a trei numere naturale consecutive este divizibil nu numai prin 3 (ceea ce este firesc), ci și prin 6, adică prin $1 \cdot 2 \cdot 3$. Tot astfel produ-

sul a cinci numere naturale consecutive este divizibil nu numai prin 5, ci și prin 120, adică prin $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5$. Rămîne ca cititorul să demonstreze că produsul a patru numere naturale consecutive se împarte prin $1 \cdot 2 \cdot 3 \cdot 4 = 24$. În concluzie, are loc următoarea teoremă generală: *Produsul a m numere naturale consecutive*

$$k(k+1)(k+2) \dots (k+m-1)$$

se împarte fără rest prin produsul primelor m numere naturale consecutive, adică prin

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot \dots \cdot (m-1)m.$$

Demonstrația elementară a acestei teoreme este destul de laborioasă. De aceea nu ne vom ocupa de ea. Pentru cititorii care cunosc analiza combinatorie și binomul lui Newton, amintim următoarele: cîtul $\frac{k(k+1)(k+2) \dots (k+m-1)}{1 \cdot 2 \cdot 3 \cdot \dots \cdot (m-1)m}$ este egal cu numărul de combinări a $(k+m-1)$ elemente, luate cîte m sau cu coeficientul termenului al $(m+1)$ -lea din dezvoltarea binomului $(a+b)^{k+m-1}$. Prin urmare, acest cît trebuie să fie un număr întreg; deci $k(k+1) \dots (k+m-1)$ trebuie să fie divizibil prin $1 \cdot 2 \cdot 3 \cdot \dots \cdot (m-1)m$.

În exemplele studiate am căutat divizorii concreți ai unor expresii pentru o valoare oarecare (întreagă) a numărului m , care intervine în aceste expresii. Adeseori problema se pune altfel: se dă o expresie și se cere să stabilim dacă ea poate avea, în general, divizori (diferiți de expresia însăși și de unitate) pentru m arbitrar sau dacă este întotdeauna un număr prim. Astfel de expresii au fost studiate în speranța că se vor găsi criteriile care să stabilească dacă un număr este prim sau nu, ținînd seama de aspectul sau structura sa. Ca exemplu poate servi o teoremă foarte simplă descoperită de matematiciana franceză Sophie Germain. Această teoremă se enunță astfel: „Orice număr de forma $m^4 + 4$, unde $m > 1$, este un număr neprim”.

Să o demonstrăm. Avem:

$$\begin{aligned} m^4 + 4 &= m^4 + 4m^2 + 4 - 4m^2 = (m^2 + 2)^2 - (2m)^2 = \\ &= (m^2 + 2 - 2m)(m^2 + 2 + 2m) = [(m-1)^2 + 1][(m+1)^2 + 1]. \end{aligned}$$

Pentru m întreg, ambii factori sînt numere întregi. Pentru $m > 1$, nici unul dintre ei nu este egal cu 1, deci $m^4 + 4$ nu va fi un număr prim. Pentru $m = 1$ apare o excepție: $m^4 + 4 = 1^4 + 4 = 5$ este număr prim.

Numerele prime îi preocupă pe matematicieni de milenii. În urmă cu 2500 de ani, ele au făcut obiectul preocupărilor matematicienilor greci. Mulți s-au străduit să găsească criterii după care să se poată stabili dacă un număr este prim sau nu, cercetînd numai structura acestuia. Primul care a reușit să înregistreze un oarecare succes pe această cale a fost Fermat. În 1640 el a demonstrat o teoremă care l-a uimit și l-a bucurat într-atîta, încît a scris în legătură cu descoperirea ei (într-o scrisoare către Frenicle): „Am fost învăluit într-o lumină strălucitoare“.

În ce consistă această teoremă a lui Fermat?

Deja am constatat că, oricare ar fi m , binomul $m^3 - m$ este divizibil prin 3, iar binomul $m^5 - m$ prin 5. Fermat a arătat că oricare ar fi numărul prim p , binomul $m^p - m$ este divizibil prin p , oricare ar fi numărul m . Acest rezultat modest a dus la generalizări importante și a provocat apariția unei literaturi matematice considerabile; el este considerat drept una dintre principalele teoreme ale teoriei numerelor. Și totuși această teoremă se numește „mica teoremă a lui Fermat“, spre deosebire de „marea teoremă a lui Fermat“ despre care a fost vorba la sfîrșitul capitolului VII.

Fermat a enunțat teorema puțin deosebit de modul în care am expus-o noi. Se observă că expresia $m^p - m$ poate fi transformată scoțîndu-l pe m în factor comun; rezultă: $m(m^{p-1} - 1)$. Dacă m este multiplu de p , teorema este evidentă și nu mai trebuie demonstrată. Prezintă importanță numai cazul cînd m nu este divizibil prin p . În acest caz, însă, m și p sînt numere prime între ele, deoarece numai numerele care sînt multipli ai numărului prim p pot avea factori comuni cu el. Urmează că diferența $m^{p-1} - 1$ trebuie să fie divizibilă prin p . Cu aceste considerații, să trecem la enunțul dat de Fermat teoremei sale: „Dacă p este prim, iar m nu se împarte prin p , atunci $m^{p-1} - 1$ este divizibil prin p “.

În limbajul congruențelor aceasta revine la: Dacă $m^{p-1} - 1$ este divizibil prin p , înseamnă că m^{p-1} și 1 sînt congruente față de modulul p , ceea ce se scrie:

$$m^{p-1} \equiv 1 \pmod{p}.$$

În această formă figurează teorema lui Fermat în cursurile moderne de teoria numerelor.

Să analizăm cîteva exemple. Luăm $m=2$; în acest caz vom putea lua drept p orice număr prim impar, adică orice număr

prim, cu excepția lui 2. În tabela următoare sînt date valorile lui p , 2^{p-1} , $2^{p-1} - 1$ și se arată că $2^{p-1} - 1$ conține totdeauna factorul p .

$$m=2$$

p	3	5	7	11	13	17
2^{p-1}	4	16	64	1 024	4 096	65 536
$2^{p-1} - 1$	$3=3 \cdot 1$	$15=5 \cdot 3$	$63=7 \cdot 9$	$1 023=11 \cdot 93$	$4 095=13 \cdot 315$	$65 535=17 \cdot 3 855$

Dacă p nu este prim (de exemplu $p=15=5 \cdot 3$), numărul $2^{p-1} - 1$ nu se va bucura neapărat de această proprietate. În adevăr, $2^{15-1} - 1 = 2^{14} - 1 = 16 384 - 1 = 16 383$ nu se împarte prin 15. Tot astfel m nu trebuie să se împartă prin p . Menținînd condiția $m=2$, dacă vom lua pentru p tot 2, nu ajungem la nici un rezultat: $2^{2-1} - 1 = 1$ nu este divizibil prin 2.

Dăm tabela următoare, în care s-au luat pentru m și alte valori:

	$m=3$	$m=5$	$m=10$
$p=2$	$3^{2-1} - 1 = 2 = 2 \cdot 1$	$5^{2-1} - 1 = 4 = 2 \cdot 2$	—
$p=3$	—	$5^{3-1} - 1 = 24 = 3 \cdot 8$	$10^{3-1} - 1 = 99 = 3 \cdot 3$
$p=5$	$3^{5-1} - 1 = 80 = 5 \cdot 16$	—	—
$p=7$	$3^{7-1} - 1 = 728 = 7 \cdot 104$	$5^{7-1} - 1 = 15 624 = 7 \cdot 2 232$	$10^{7-1} - 1 = 999 999 = 7 \cdot 142 857$
$p=11$	$3^{11-1} - 1 = 59 048 = 11 \cdot 5 368$	$5^{11-1} - 1 = 9 765 624 = 11 \cdot 887 784$	$10^{11-1} - 1 = 9 999 999 999 = 11 \cdot 909 090 909$

Se vede că m nu trebuie să fie obligatoriu prim (de exemplu în coloana a treia $m=10=2 \cdot 5$). Condiția care se impune este ca m să nu fie divizibil prin p . De aceea pentru $m=3$ nu am considerat valoarea $p=3$, pentru $m=5$ valoarea $p=5$, pentru $m=10$ valorile $p=2$ și $p=5$. Efectuînd calculele necesare, cititorul se va convinge singur că în aceste cazuri teorema nu se confirmă.

Vom demonstra acum teorema lui Fermat. Începem prin a considera sistemul complet al resturilor pozitive minime ale nu-

mărilor p , adică toate resturile care se pot obține împărțind diverse numere prin p (în afară de restul nul). Acestea sînt:

$$1, 2, 3, \dots, p-2, p-1. \quad (1)$$

Să înmulțim fiecare dintre ele cu numărul m , nedivizibil prin p . Rezultă:

$$1m, 2m, 3m, 4m, \dots, (p-2)m, (p-1)m. \quad (2)$$

Toate numerele din (2) sînt distincte și nici unul nu este egal cu zero; la împărțirea prin p , toate dau resturi diferite. În adevăr, dacă am și bm dau la împărțirea prin p resturi egale [a și b fiind numere distincte din (1), neapărat mai mici decît p], diferența $am - bm = m(a - b)$ trebuie să se împartă prin p . Numerele m și p sînt prime. Prin urmare, $a - b$ trebuie să se împartă prin p , ceea ce este însă imposibil, pentru că diferența $a - b$ este mai mică decît p (a și b sînt numere pozitive mai mici decît p). Contradicția la care am ajuns arată că ipoteza inițială este greșită. Prin urmare nu se obțin resturi egale; toate resturile sînt distincte și egale cu numerele primului șir (cu $1, 2, 3, \dots, p-1$), luate într-o altă ordine.

Dar aceasta înseamnă că fiecare număr din șirul (2) este congruent față de modulul p (dă același rest) cu unul și numai cu unul dintre numerele șirului (1). Notăm cu litera k_1 acel număr din șirul (2) care este congruent cu 1, cu k_2 numărul congruent cu 2 etc., cu k_{p-1} numărul congruent cu $p-1$. Obținem următorul șir de congruențe:

$$\left. \begin{array}{l} k_1 \equiv 1 \\ k_2 \equiv 2 \\ k_3 \equiv 3 \\ \dots \\ k_{p-2} \equiv p-2 \\ k_{p-1} \equiv p-1 \end{array} \right\} \pmod{p}.$$

Să înmulțim între ele toate congruențele din acest șir, ceea ce este permis. Rezultă:

$$k_1 k_2 \dots k_{p-1} \equiv [1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1)] \pmod{p}. \quad (I)$$

Trecem la punctul central al demonstrației.

Numerele $k_1, k_2, \dots, k_{p-1}$ sînt de fapt toate numerele șirului (2), luate într-o altă ordine. Produsul lor nu depinde de ordinea factorilor; deci avem:

$$k_1 k_2 \dots k_{p-1} = 1m \cdot 2m \cdot 3m \dots (p-1)m = m^{p-1} \cdot 1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1).$$

Înlocuind primul membru al congruenței (I) prin mărimea egală cu el, din expresia aceasta rezultă:

$$m^{p-1} \cdot 1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1) \equiv [1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1)] \pmod{p}.$$

Toți factorii produsului $1 \cdot 2 \cdot \dots \cdot (p-1)$ sînt mai mici decît numărul inițial p și sînt primi cu el. Prin urmare putem simplifica congruența cu aceste numere. Obținem:

$$m^{p-1} \equiv 1 \pmod{p},$$

ceea ce trebuia demonstrat.

Demonstrația se poate face fără a recurge la noțiunea de congruență, dar este foarte laborioasă. Așa a procedat și Fermat, care a trăit cu aproape 200 de ani înaintea lui Gauss, inventatorul teoriei congruențelor. Există o demonstrație interesantă a teoremei lui Fermat (legată de transformarea unei fracții simple într-o fracție zecimală periodică), dar ea este lungă și nici nu se potrivește prea bine cu tema cărții noastre, care se ocupă de numerele întregi ¹⁾.

Cititorilor familiarizați cu binomul lui Newton le putem da încă o demonstrație a teoremei lui Fermat. Iată în ce consistă ea.

Să scriem dezvoltarea binomului $(m+1)^p$ după formula lui Newton, unde m este întreg, iar p prim:

$$(m+1)^p = m^p + pm^{p-1} + \frac{p(p-1)}{1 \cdot 2} m^{p-2} + \dots + pm + 1.$$

Toți coeficienții binomului lui Newton, adică toate numerele de forma $\frac{p(p-1) \dots (p-k+1)}{1 \cdot 2 \cdot 3 \cdot \dots \cdot k}$ sînt întregi. Mai mult, în afară de primul și de ultimul, ei sînt toți multipli de p . În adevăr, știm că în fracția $\frac{p(p-1) \dots (p-k+1)}{1 \cdot 2 \cdot 3 \cdot \dots \cdot k}$ numerele de la numitor trebuie să se simplifice în întregime cu factorii numărătorului. Însă p este prim cu toate numerele $1, 2, 3, \dots, k$; deci aceste numere trebuie să se simplifice în întregime cu factorii produsului $(p-1) \cdot (p-2) \dots (p-k+1)$; factorul p rămîne. Așadar, avem egalitatea

$$(m+1)^p = m^p + (\text{un număr divizibil prin } p) + 1,$$

care exprimă următoarele: dacă binomul $m^p - m$ este divizibil prin p , pentru o valoare a lui m , atunci va fi în mod necesar divi-

¹⁾ Demonstrația respectivă este expusă în interesanta carte a lui Rade-macher și Toeplitz „Von Zahlen und Figuren”, Ed. Julius Springer, 1933.

zibilă prin p și expresia $(m+1)^p - (m+1)$. Ultima expresie este un binom asemănător cu primul, însă avînd baza cu o unitate mai mare (pentru că din divizibilitatea scăzătorului și restului printr-un număr oarecare, rezultă că și descăzutul este divizibil prin acest număr). Dacă $m=1$, atunci $m^p - m = 1 - 1 = 0$ și se împarte cu siguranță prin p , zero fiind divizibil prin orice număr. Așadar și $(m+1)^p - (m+1)$, adică $2^p - 2$, va fi divizibil prin p ; rezultă că $3^p - 3$ este de asemenea divizibil prin p etc., pînă la o valoare arbitrară a lui m^1). Prin urmare, pentru m arbitrar și p prim, $m^p - m$ este divizibil prin p („mica” teoremă a lui Fermat).

Fermat a descoperit această teoremă căutînd expresii care să conțină litera n și care să fie numere prime. Referitor la ultima problemă, Fermat a enunțat o „teoremă” interesantă care s-a dovedit a fi greșită (v. p. 80).

El a considerat numerele de forma $2^{2^n} + 1$, unde n este un întreg arbitrar.

Luînd n egal cu 0, 1, 2, 3, 4 a obținut numerele din următoarea tabelă:

n	0	1	2	3	4
$2^{2^n} + 1$	$2^1 + 1 = 3$	$2^2 + 1 = 5$	$2^4 + 1 = 17$	$2^8 + 1 = 257$	$2^{16} + 1 = 65\,537$

Toate numerele din linia a doua (3, 5, 17, 257, 65 537) sînt prime. Fermat a afirmat că și pentru valori mai mari ale lui n se vor obține numere prime. Pentru $n=5$, Fermat a obținut numărul 4 294 967 297, pe care n-a mai fost în stare să-l descompună în factori și a crezut că este prim. Euler a găsit însă că 4 294 967 297 este divizibil prin 641, adică nu este prim. El a arătat astfel că Fermat greșise²⁾.

Această propoziție greșită este foarte instructivă. Uneori matematicienii talentați au un „simț” special care le sugerează în

¹⁾ Reamintim că un astfel de raționament se numește raționament prin inducție matematică completă.

²⁾ Este ușor de împărțit 4 294 967 297 prin 641, dacă știm dinainte că trebuie să împărțim acest număr prin 641. Însă a împărți un număr de zece cifre rînd pe rînd toate numerele prime (numai în prima sută de numere sînt 25 de numere prime), fără a dispune nici de tabele destul de mari pentru numerele prime, nici de alte numere ajutătoare, este o muncă foarte dificilă.

ce direcție să-și facă cercetările. În capitolul următor vom constata că numerele lui Fermat (numerele prime de forma $2^{2^n} + 1$) s-au dovedit deosebit de remarcabile și că studiul lor a dus ulterior la descoperiri importante. Mai departe, matematicianul lucrează ca orice cercetător al naturii: face presupuneri (ipoteze), le verifică prin observație și printr-un fel de „experiență” matematică, el caută analogii etc. Însă după ce a obținut un rezultat în baza unei intuiții sau a unei „experiențe”, matematicianul este obligat să-l demonstreze riguros. În caz contrar există pericolul ca afirmația enunțată să se dovedească greșită.





CAPITOLUL XI

CIURUL LUI ERATOSTENE



În capitolele precedente am întâlnit deseori numere prime. Am spus că se numește prim un număr care se divide numai cu el însuși și cu unu. Numărul 1 nu are decât un singur divizor și nu face parte dintre numerele prime. Numerele 2, 3, 5, 7, 11 sînt evident prime. Dimpotrivă, numerele 4, 6, 8, 9 nu sînt prime.

Înainte de a considera problemele generale legate de numerele prime, să cercetăm numerele prime de la 1 pînă la 1000 și să observăm proprietățile lor cele mai simple.

Cum vom afla toate numerele prime pînă la 1000? Procedăm în modul următor: scriem toate numerele de la 1 pînă la 1000. Tăiem pe 1 (care nu este număr prim). Tăiem apoi toate numerele multipli de 2 (numerele pare); cu alte cuvinte tăiem toate numerele din două în două; obținem o tabelă de forma:

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.

Apoi, subliniem următorul număr netăiat după 2 (adică 3) și tăiem fiecare al treilea număr (numerele care sînt multipli de 3); după aceea subliniem pe 5 (4 a fost tăiat înainte) și tăiem

fiecare al cincilea număr (numerele multipli de 5) etc. Obținem următoarea tabelă:

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.

În felul acesta vom tăia toate numerele neprime și vom obține tabela numerelor prime (dată în anexă la sfîrșitul cărții).

O astfel de tabelă a fost întocmită pentru prima dată de matematicianul grec Eratostene (sec. III î.e.n.). El a scris numerele pe un papyrus întins pe un cadru și a găurit locurile unde erau numere neprime, în loc să le taie cum am făcut noi. A obținut ceva asemănător cu un ciur, prin care au fost „strecurate” toate numerele neprime, iar cele prime au rămas. De aceea tabela numerelor prime a rămas pînă astăzi sub denumirea de „ciurul lui Eratostene”.

Examinînd ciurul lui Eratostene, observăm că numerele prime sînt mult mai frecvente la începutul tabelii decît, de exemplu, în apropierea lui 1000. Astfel, de la 1 pînă la 10 întîlnim patru numere prime: 2, 3, 5, 7. În schimb, între numerele prime 997 și 1009 există 11 numere neprime consecutive. Dacă vom merge mai departe, vom întîlni un șir de numere oricît de lung, format în întregime din numere neprime consecutive.

De exemplu să demonstrăm că există un șir de numere format din o sută de numere neprime consecutive. Pentru aceasta să considerăm numărul reprezentat prin produsul tuturor numerelor naturale de la 1 pînă la 101:

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot \dots \cdot 99 \cdot 100 \cdot 101.$$

Acesta este un număr foarte mare. El este egal aproximativ cu $95 \cdot 10^{158}$, adică este cu mult mai mare decît numerele „astro-nomice” obișnuite, însă neglijabil de mic în comparație cu numărul 9^{99} , de care ne-am ocupat la p. 14. Să notăm acest număr cu litera A . Să considerăm șirul de numere

$$A+2, A+3, A+4, A+5, \dots, A+99, A+100, A+101.$$

Acesta este un șir compus din o sută de numere întregi consecutive. Nici unul dintre ele nu este prim. De exemplu $A+2$ se divide

prin 2. În adevăr, A este divizibil prin 2, deoarece, prin ipoteză, conține factorul 2. Al doilea termen (numărul 2) este evident divizibil prin 2; deci suma lor se va împărți prin 2, adică $A+2$ nu va fi un număr prim. Tot astfel $A+3$ va fi divizibil prin 3, $A+4$ prin 4 etc., în sfârșit $A+101$ va fi divizibil prin 101, pentru că A conține factorul 101. Așadar toate numerele din șirul obținut sînt neprime, ceea ce voiam să demonstrăm.

În același mod se demonstrează că putem găsi un șir oricît de mare (care conține, dacă vrem, o mie sau un milion de numere), format numai din numere neprime.

Apar în mod firesc unele întrebări: poate că, începînd de la un anumit număr, toate numerele sînt neprime? Poate că există numai un număr finit de numere prime, iar celelalte numere, pînă la infinit, sînt neprime? Poate că există un număr prim care este cel mai mare? Ce fel de număr este acesta?

Astfel de întrebări i-au preocupat încă pe matematicienii din antichitate. Euclid a studiat această problemă și a dat soluția ei completă. El a reușit să demonstreze că numerele prime sînt în număr infinit, că nu există un număr prim care să fie cel mai mare. Să demonstrăm această propoziție.

Urmînd raționamentul lui Euclid, vom demonstra propoziția cu ajutorul metodei denumite „reducere la absurd”¹⁾. Cu alte cuvinte, admițînd că există un număr prim care este cel mai mare, vom ajunge în urma unor raționamente corecte la o contradicție. Aceasta ne va arăta că ipoteza de la care am pornit este greșită și deci un astfel de număr nu există.

Așadar, să presupunem că există un număr prim cel mai mare. Îl vom nota cu p . Să considerăm numărul format din produsul tuturor numerelor prime, adică numărul $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot \dots \cdot p$. Adăugînd 1 la acest număr, obținem $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot \dots \cdot p + 1$, care este, bineînțeles, considerabil mai mare decît p .

Să încercăm a împărți numărul $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot \dots \cdot p + 1$ printr-un număr prim. Observăm că $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot \dots \cdot p + 1$ este format din doi termeni. Primul termen $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot \dots \cdot p$, ca produs al tuturor numerelor prime, este divizibil prin orice număr prim, iar al doilea termen (numărul 1) împărțit prin orice număr întreg, în afară de 1, dă cîtul zero și restul 1. Prin urmare și suma $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot \dots \cdot p + 1$ va da restul 1, dacă o vom împărți prin orice număr prim.

¹⁾ Actualmente există multe demonstrații diferite care arată că mulțimea numerelor prime este infinită.

Deci, admițînd că p este cel mai mare număr prim, am ajuns la o contradicție; în acest caz, numărul format de noi nu se împarte prin nici un număr prim.

Prin urmare, numărul $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot \dots \cdot p + 1$ ori este prim ori se împarte printr-un număr prim distinct de $2, 3, 5, 7, 11, \dots, p$ și deci mai mare decît p . Așadar, presupunînd că p este cel mai mare număr prim, am demonstrat că există un număr prim mai mare. Această concluzie contradictorie ne convinge că ipoteza inițială este greșită. Nu poate exista un număr prim care să fie cel mai mare: există deci o infinitate de numere prime.

Toate numerele prime, începînd cu 3, pot fi împărțite în două clase. Unele (de exemplu 5, 13, 17) sînt de forma $4n+1$, celelalte (de exemplu 3, 7, 11) sînt de forma $4n-1$. Un număr impar (toate numerele prime, cu excepția lui 2, sînt impare) nu poate avea altă formă, deoarece la împărțirea unui număr impar prin 4, resturile posibile sînt numai 1 și 3. Bineînțeles, nu orice număr de forma $4n \pm 1$ este prim, însă orice număr prim are una dintre aceste forme. Se pune problema: oare în fiecare din cele două clase există o infinitate de numere prime? Nu cumva una dintre ele este finită? Bineînțeles, ambele simultan nu pot fi finite.

Cercetările nu arătat că există o infinitate de numere prime în ambele clase. Pentru numerele de forma $4n+1$, demonstrația este întrucîtva greoaie; de aceea vom demonstra numai că mulțimea numerelor prime de forma $4n-1$ este infinită.

În prealabil trebuie să demonstrăm următoarea propoziție ajutătoare (lemă): „Produsul mai multor numere de forma $4n+1$ este și el un număr de forma $4n+1$.”

Fie două numere din această clasă: $4a+1$ și $4b+1$. Înmulțindu-le, obținem:

$$\begin{aligned}(4a+1)(4b+1) &= 16ab + 4a + 4b + 1 = \\ &= 4(4ab + a + b) + 1 = 4k + 1,\end{aligned}$$

unde k reprezintă numărul întreg $4ab + a + b$. Produsul are tot forma $4n+1$. Putem trage aceeași concluzie despre produsul a trei factori, a patru factori etc., în general, a unui număr oarecare de factori de acest fel.

Acum putem demonstra că mulțimea numerelor prime de forma $4n-1$ este infinită; vom aplica metoda de demonstrație a lui Euclid. Admitem propoziția contrarie, că ar exista un număr finit (m) de numere prime de forma $4n-1$. Notăm aceste numere cu $p_1, p_2, \dots, p_m$. Să considerăm numărul:

$$A = 4 \cdot p_1 \cdot p_2 \cdot \dots \cdot p_m - 1.$$

Deoarece este de forma $4n-1$ trebuie să aibă cel puțin un factor care să fie un număr prim de această formă. Dar produsul unor factori de forma $4n+1$ trebuie, de asemenea, să fie de forma $4n+1$. Așadar, printre factorii primi ai numărului A trebuie să existe un $p=4n-1$. Numărul p însă nu poate fi egal cu vreunul dintre numerele $p_1, p_2, \dots, p_m$, pentru că A nu este divizibil prin nici unul dintre aceste numere; p este un număr prim de forma $4n-1$. Prin urmare, șirul numerelor $p_1, p_2, \dots, p_m$ nu epuizează toate numerele prime de forma $4n-1$; acest rezultat contrazice ipoteza inițială. Deci există o infinitate de numere prime de forma $4n-1$.

Numerele de forma $4n-1$ formează o progresie aritmetică, primul ei termen fiind 3, iar rația 4:

$$\div 3, 7, 11, 15, \dots$$

Teorema demonstrată putea fi enunțată și astfel: *progresia aritmetică infinită*

$$\div 3, 7, 11, 15, 19, \dots$$

conține o infinitate de numere prime.

Există oare și alte progresii cu aceeași proprietate? Am văzut că progresia în care primul termen este 1 și rația 1 (adică șirul numerelor naturale) conține o infinitate de numere prime. Același lucru s-a spus (fără demonstrație) și despre progresia $\div 1, 5, 9, 13, 17, 21, \dots$, adică despre numerele de forma $4n+1$.

Problema: câte numere prime sînt într-o anumită progresie aritmetică a preocupat pe mulți matematicieni, în special la începutul secolului al XIX-lea. Ea a fost rezolvată în întregime de către Lejeune-Dirichlet (1805—1859) care a demonstrat că orice progresie aritmetică în care primul termen și rația sînt numere prime între ele conține o infinitate de numere prime. Condiția ca primul termen și rația să fie prime între ele este esențială: dacă aceste numere au un factor comun diferit de 1, este evident că toți termenii progresiei vor conține acest factor și deci nu vor mai fi numere prime.

Este imposibil să expunem elementar demonstrația lui Dirichlet. Vom considera încă o problemă care se ivește la examinarea atentă a ciurului lui Eratostene și care a rămas nerezolvată. Printre numerele prime se înțelnesc perechi formate din numere impare vecine, prime între ele. Astfel sînt numerele 5 și 7, 11 și 13, 17 și 19 etc. Perechile de acest gen apar destul de frecvent la începutul „ciurului”, însă pe măsură ce înaintăm spre numerele mari

ele devin tot mai rare. Între 1 și 100 sînt opt perechi de acest fel (3 și 5; 5 și 7; 11 și 13; 17 și 19; 29 și 31; 41 și 43; 59 și 61; 71 și 73); între numerele 501 și 600 sînt numai două perechi (521 și 523; 569 și 571). Mai departe ele apar cu totul neuniform și din ce în ce mai rar (considerabil mai rar decît numerele prime). De altfel se cunosc și „perechi” cu totul impresionante, cum ar fi 5971847 și 5971849. Se pune întrebarea: există oare printre aceste perechi una care să fie ultima? Pînă în prezent aceasta nu s-a putut stabili. Mai mult, nu s-a conturat nici măcar o metodă cu ajutorul căreia să ne putem apropia de soluție.

Ne vom referi acum la posibilitatea descompunerii oricărui număr în factori primi, care constituie cea mai importantă problemă referitoare la numerele prime. Aceasta revine la a reprezenta în mod unic orice număr sub forma unui produs de numere prime, ceea ce ni se pare cu totul evident. În realitate, însă, poziția referitoare la descompunerea în factori primi este o teoremă atît de importantă în teoria numerelor, încît este deseori denumită „teorema fundamentală a aritmeticii”. Iată enunțul ei: „Orice număr natural se descompune în mod unic în factori primi”. Să demonstrăm această teoremă.

Vom demonstra în prealabil următoarea leamnă: divizibilitatea produsului kl prin numărul prim p conduce la concluzia că cel puțin unul dintre factori (fie k , fie l sau și unul și celălalt) se împarte prin p .

În adevăr, numărul k sau se divide prin p (și atunci teorema este demonstrată) sau nu se divide. Dacă numărul k nu este divizibil prin p , atunci numerele k și p sînt prime între ele, deoarece k nu conține printre factorii săi numărul p , iar p (prim) nu are alți factori în afară de 1 și de el însuși. În cazul cînd p și k sînt primi, iar produsul kl este divizibil prin p , atunci l trebuie să se împartă prin p (teorema a treia din cap. VI, p. 50). Prin urmare l se divide prin p .

Această leamnă se extinde fără dificultate la orice număr de factori: *dacă produsul $ab \dots h$ este divizibil prin numărul prim p , atunci cel puțin unul dintre numerele $a, b, \dots, h$ este divizibil prin p .*

Trecem acum la demonstrarea teoremei fundamentale a aritmeticii. Vom demonstra că orice număr natural se descompune în factori primi în mod unic. De fapt trebuie să demonstrăm două afirmații: 1) posibilitatea descompunerii în factori primi și 2) unicitatea acestei descompuneri.

Posibilitatea descompunerii în factori este evidentă. Fie dat un număr arbitrar N . Pentru N prim, teorema este demonstrată, deoarece el însuși poate fi considerat unicul său factor prim. Dacă însă N nu este prim, el se divide printr-un număr prim p , mai mic decât N . Vom obține citul N_1 , de asemenea mai mic decât N . Dacă N_1 este prim, atunci $N = p_1 N_1$ și teorema este demonstrată. Când N_1 nu este prim, atunci el se împarte printr-un număr prim p_2 , mai mic decât N_1 , și se obține citul N_2 , de asemenea mai mic decât N_1 . Numerele $N_1, N_2, N_3, \dots$ sînt descrescătoare și numărul lor nu poate fi infinit. De aceea vom ajunge la un ultim cit, la p_m , care va fi prim; vom obține reprezentarea numărului N sub forma unui produs de numere prime $p_1 p_2 \dots p_m$.

Toate considerațiile acestea sînt foarte simple și aproape evidente. Esențială este partea a doua a teoremei: afirmația că descompunerea în factori primi a lui N este unică. Să presupunem că am reușit să descompunem numărul N în factori primi prin două metode: prima metodă a dat descompunerea

$$N = p_1 p_2 \dots p_r,$$

iar a doua descompunerea

$$N = q_1 q_2 \dots q_s,$$

unde $p_1, p_2, \dots, p_r$ și $q_1, q_2, \dots, q_s$ sînt numere prime.

Evident, avem:

$$p_1 p_2 \dots p_r = q_1 q_2 \dots q_s. \quad (I)$$

Membrul întii al acestei egalități este divizibil prin p_1 ; deci și membrul al doilea (produsul $q_1 q_2 \dots q_s$) va fi divizibil prin p_1 . În virtutea lemei demonstrate, trebuie ca unul dintre factorii $q_1, q_2, \dots, q_s$ să se împartă prin p_1 . Să admitem că q_1 se împarte prin p_1 . Deoarece q_1 este prim, el se împarte numai prin 1 și prin el însuși; deci avem:

$$q_1 = p_1.$$

Împărțind ambii membri ai egalității (I) prin $p_1 = q_1$, obținem:

$$p_2 p_3 \dots p_r = q_2 q_3 \dots q_s.$$

Repetind raționamentul, ajungem la concluzia că

$$q_2 = p_2,$$

iar după o nouă simplificare, la relația:

$$p_3 p_4 \dots p_r = q_3 q_4 \dots q_s.$$

Tot astfel găsim $q_3 = p_3, q_4 = p_4, \dots, q_s = p_s$. Prin urmare avem tot atîția factori q , cîți și p ; fiecare q este egal cu cîte un p , adică cele două descompuneri ale numărului N în factori primi sînt identice.

Cititorii își amintesc din școala medie cum se descompune practic un număr în factori primi. De exemplu descompunerea în factori primi a numărului 8316 se efectuează astfel:

8316	2
4158	2
2079	3
693	3
231	3
77	7
11	11

adică

$$8316 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3 \cdot 7 \cdot 11 = 2^2 \cdot 3^3 \cdot 7 \cdot 11.$$

Prin urmare, orice număr N poate fi reprezentat în mod unic sub forma:

$$N = p_1^{\alpha} p_2^{\beta} \dots p_m^{\lambda},$$

unde $p_1, p_2, \dots, p_m$ sînt numere prime, iar $\alpha, \beta, \dots, \lambda$ sînt anumiți exponenți. Această reprezentare a numărului N este denumită cîteodată „descompunere canonică în factori“.

Înainte de a încheia discuția referitoare la teorema fundamentală a aritmeticii, mai facem o remarcă. Am definit numărul prim ca numărul care nu are alți divizori decât pe el însuși și unitatea. Mai departe am arătat că dacă produsul mai multor numere este divizibil printr-un număr prim, atunci cel puțin unul dintre factori va fi divizibil prin acest număr prim (lema la teorema fundamentală). Am fi putut demonstra teorema reciprocă a acestei leme: anume că orice număr prin care se împarte în mod necesar cel puțin unul dintre factorii unui produs de mai multe numere nu are alți factori în afară de unitate și de el însuși. Această ultimă proprietate poate fi adoptată ca definiție a numerelor prime. Așa se procedează de multe ori: se numește număr prim numărul cu care se poate împărți un produs numai în cazul în care cu el se împarte unul din factori; un număr care nu are alți factori în afară de el însuși și de unitate se numește indecompozabil. Folosind acești termeni, putem enunța lema noastră astfel: „Orice număr indecompozabil este prim“. Reciproca este: „Orice număr prim este indecompozabil“. Ambele enunțuri pot

fi reunite: termenii „număr prim” și „număr indecompozabil” înseamnă același lucru.

Cititorul obișnuit cu diversele surprize ale aritmeticii nu va întreba oare: „de ce a fost necesar să se introducă doi termeni, dacă ei înseamnă același lucru?” Desigur cititorul simte că aici se ascunde un „ce”. În adevăr, dacă există „aritmetici” în care trei ori trei fac patru și $3 \cdot 3 = 10$, de ce să nu existe și o aritmetică în care numerele prime să nu fie indecompozabile, iar cele indecompozabile să nu fie prime?...

Este drept, o astfel de aritmetică pare imposibilă! În adevăr, tocmai lema al cărei sens consistă, în fond, în identificarea noțiunilor de prim și indecompozabil ne-a permis să demonstrăm că descompunerea în factori primi a oricărui număr este unică. Să fie oare posibile „aritmetici” în care același număr să se poată descompune în factori indecompozabili pe mai multe căi diferite, adică să aibă mai multe descompuneri canonice?

Este posibil! Există sisteme de numere în care descompunerea în factori indecompozabili nu este unică, iar descompunerea în factori primi nu este întotdeauna posibilă. Tocmai existența acestor sisteme a dus la necesitatea de a distinge numerele prime de cele indecompozabile. Fără îndoială, sistemele de numere care au dus la stabilirea acestor noțiuni sînt foarte complicate și nu avem posibilitatea să ne ocupăm de ele aici, deși prezintă multă importanță pentru teoria numerelor. Vom considera însă un exemplu artificial, simplu, care ne va ajuta să ne orientăm în fondul problemei.

Fie șirul tuturor numerelor pozitive pare, adică numerele:

2, 4, 6, 8, 10, 12, 14, 16, 18...

Acest șir seamănă, prin multe dintre proprietățile sale, cu șirul numerelor naturale. De exemplu se pot efectua întotdeauna adunarea și înmulțirea acestor numere; aceasta înseamnă că suma și produsul a două sau a mai multe numere pare dau tot numere pare. Scăderea unui număr mai mic din unul mai mare este de asemenea întotdeauna posibilă. În sfîrșit, împărțirea cu rest (scăderea consecutivă) este în totul analogă împărțirii cu rest obișnuită.

În acest sistem unele numere au numai doi divizori (se consideră, bineînțeles, numai divizorii pari).

Astfel sînt numerele 4, 6, 10, 14 etc., care se împart numai prin 2 și prin ele însele. Orice număr de forma $4n+2$ (unde n

este un număr natural obișnuit) va avea numai doi divizori. Din punctul de vedere al sistemului considerat, numerele acestea vor fi indecompozabile. Analog cu numărul 1 din șirul natural, numărul 2 are aici doar un singur divizor (pe el însuși). În sfîrșit, numerele 8, 12, 16 (în general, numerele de forma $4n$) au mai mulți divizori.

Deocamdată analogia cu șirul natural este completă. Dar mai departe încep nepotrivirile. Să considerăm numărul 420 din acest sistem. El poate fi descompus în factori pe două căi, factorii fiind indecompozabili din punctul de vedere al sistemului nostru. În adevăr, avem: $420 = 6 \cdot 70$ și $420 = 14 \cdot 30$. Numerele 6, 14, 30 și 70 sînt indecompozabile (nici unul dintre ele nu este produsul a două numere pare). Prin urmare sînt posibile două descompuneri ale numărului 420 în factori care nu mai sînt decompozabili.

Care numere vor juca rolul de numere prime în sistemul nostru? Nu este greu să ne dăm seama că acestea vor fi numerele de forma $2p$, unde p este prim în sens obișnuit (din punctul de vedere al aritmeticii șirului numerelor naturale). În sistemul nostru orice număr prim va fi indecompozabil. Însă nu orice număr indecompozabil va fi prim. Numerele 30, 42, 70, care sînt indecompozabile, nu vor fi prime. Lemma care precede teorema fundamentală a aritmeticii nu este verificată pentru ele. De aceea am putut descompune un număr în factori indecompozabili pe mai multe căi.

Acest sistem de numere prezintă și un alt paradox: nu orice număr poate fi descompus în factori primi; deci nu orice număr va putea fi reprezentat ca produsul unor numere de tipul $2p$, unde p este un număr prim în sens obișnuit. Numărul 420, care poate fi descompus pe două căi în factori indecompozabili, nu poate fi descompus în factori primi.

Pentru a încheia capitolul consacrat ciurului lui Eratostene, vom spune cîteva cuvinte despre încercările de a găsi o formulă generală care să dea numai numere prime pentru toate valorile întregi ale mărimii n pe care o cuprinde. „Vinătoarea” după asemenea formule a început încă din antichitate și nu a fost încununată de succes nici pînă în prezent. Există diferite formule în care intervine o anumită mărime n și care dau numere prime pentru diferite valori întregi ale lui n . Însă, pentru o anumită valoare a lui n , toate „își încetează funcțiunea”. De exemplu expresia

$$A = n^2 - 79n + 1601$$

dă numere prime pentru orice n mai mic decît 79. Pentru $n=0$, obținem $A=1601$, pentru $n=1$ avem $A=1523$, pentru $n=2$ găsim $A=1447$, care sînt toate prime. În sfîrșit pentru $n=39$ obținem $A=41$, tot un număr prim. Mai departe, pentru valori ale lui n cuprinse între 40 și 79, obținem aceleași valori ale lui A , însă în ordine inversă: pentru $n=40$ avem $A=41, \dots$, pentru $n=78$ avem $A=1523$, pentru $n=79$ avem $A=1601$. Pentru $n=80$, însă, formula „face nazuri“! În acest caz obținem:

$$A=80^2-79 \cdot 80+1601=1681=41^2,$$

care nu este număr prim.

Iată un alt exemplu interesant¹⁾. Dacă în expresia

$$N = \frac{2^p + 1}{3}$$

vom substitui în locul lui p diferitele numere prime impare pînă la 31, valorile lui N vor fi și ele prime. Dăm mai departe tabela valorilor lui p și a valorilor corespunzătoare ale lui N .

p	$N = \frac{2^p + 1}{3}$	p	$N = \frac{2^p + 1}{3}$
3	3	17	43 691
5	11	19	174 761
7	43	23	2 796 203
11	683	29	178 956 771
13	2 731	31	715 827 883

Pentru $p=37$ formula „refuză să funcționeze“; în acest caz obținem $N = \frac{2^{37} + 1}{3} = 45\,812\,984\,491$, care nu este prim; acest număr se descompune în doi factori primi, și anume:

$$45\,812\,984\,491 = 1\,777 \cdot 25\,781\,083.$$

La sfîrșitul capitolului precedent am amintit celebra eroare a lui Fermat, legată de „vînătoarea de formule“, care să dea numere prime. Fermat a crezut că, pentru orice n întreg și nenegativ, expresia $2^{2^n} + 1$ este un număr prim. Dacă simțul matematic l-a trădat pe Fermat în ceea ce privește valabilitatea afirmației, el

¹⁾ Acest exemplu mi-a fost indicat de prof. A. F. Bermant.

l-a condus totuși spre o problemă foarte importantă și interesantă. S-a constatat că dacă nu toate numerele de forma $2^{2^n} + 1$ sînt prime, în schimb cele dintre ele care sînt prime se bucură de unele proprietăți remarcabile. Am mai arătat că aceste numere au fost studiate de Euler, care a descoperit greșeala lui Fermat. Însă cel mai interesant rezultat a fost obținut de Gauss. El se leagă de o cunoscută problemă de geometrie: construcția unor poligoane regulate cu ajutorul riglei și al compasului.

Oamenii din antichitate știau să construiască triunghiuri, patrulatere și pentagoane regulate. Folosind posibilitatea de a împărți în două părți egale orice unghi, se construiau cu ușurință poligoane cu 8, 16 și, în general, cu 2^n laturi; de asemenea poligoane cu 6, 12 și, în general cu $2^n \cdot 3$ laturi; cu 10, 20 și, în general, cu $2^n \cdot 5$ laturi. Scăzînd dintr-o șesime de cerc o zecime de cerc, se obținea o cincisprezecime, adică se construiau poligoane cu 15, cu 30, 60 și, în general, cu $2^n \cdot 15$ laturi. Însă toate încercările de a construi cu ajutorul riglei și al compasului un poligon regulat cu 7 sau cu 11 laturi s-au soldat prin eșecuri.

Mai mult de două mii de ani toate încercările matematicienilor de a construi cu ajutorul riglei și al compasului poligoanele regulate pe care anticii nu știau să le construiască s-au terminat printr-un eșec. Abia în anul 1796, Gauss (pe atunci în vîrstă de 19 ani) a găsit, spre surprinderea tuturor matematicienilor, un procedeu pentru construirea cu rigla și compasul a poligonului regulat cu 17 laturi, iar după cinci ani el a publicat soluția problemei poligoanelor regulate în forma ei generală.

Gauss a demonstrat următoarea teoremă remarcabilă: *cu ajutorul riglei și al compasului se pot construi numai poligoanele regulate al căror număr de laturi este „un număr prim al lui Fermat“, adică un număr de forma $2^{2^n} + 1$ (bineînțeles, pentru valorile lui n , cărora le corespund în rezultat numere prime).* De exemplu pentru $n=2$, obținem poligonul regulat cu 17 laturi, pentru $n=3$, poligonul cu 257 laturi. Dacă numărul de laturi al poligonului regulat este prim, însă nu este un număr al lui Fermat, construirea lui cu rigla și compasul este imposibilă. Poligoanele regulate cu 7, 11 și 13 laturi nu se pot construi cu ajutorul riglei și al compasului, pe cînd cele cu 17 și cu 257 laturi se pot construi!

Însuși Gauss, care a rezolvat problema în forma ei generală, a dat o metodă complet elaborată numai pentru construirea poligonului cu 17 laturi. „Numerele lui Fermat“ care urmează după 17 sînt 257 și 65 537. Construcția completă a poligonului cu 257 laturi a fost dată de Richelot (ea ocupă 80 de pagini), iar poligonul cu 65 537 laturi a fost construit după metoda lui Gauss de către Hermes (manuscrisul ocupă o valiză destul de voluminoasă și se păstrează la Göttingen). Prin urmare, teoria numerelor s-a dovedit a fi legată în modul cel mai curios de geometrie.

În semn de omagiu lui Gauss i s-a ridicat la Göttingen un monument, al cărui pedestal are forma unei prisme cu baza un poligon regulat cu 17 laturi.



CAPITOLUL XII

DES ORI RAR ?



Examinînd ciurul lui Eratostene, se observă că la început intervalele dintre numerele prime consecutive sînt mici, însă pe măsură ce înaintăm în șirul numerelor naturale ele devin, de regulă, din ce în ce mai mari, cu alte cuvinte numerele prime se întîlesc din ce în ce mai rar (v. tabela din Anexă). Între primele zece numere naturale găsim patru numere prime, în schimb între 1 001 și 1 010 nu există decît unul singur : 1 009.

Euclid a demonstrat că există o infinitate de numere prime : oricît de departe am merge în șirul numerelor naturale, totdeauna vom găsi numere prime. Pe de altă parte, „insulele“ formate în întregime din numere neprime vor deveni, de regulă, „mai lungi“, numerele prime se vor întîlni din ce în ce mai rar. Care este legea distribuției numerelor prime ? Cum să aflăm, de exemplu, cîte numere prime sînt cuprinse în intervalul dintre 1 000 000 și 10 000 000, fără a le număra direct ? Aceasta este una dintre cele mai dificile probleme și nu a fost rezolvată definitiv pînă în prezent. Dificultatea problemelor legate de distribuția numerelor prime a ajuns proverbială pentru matematicieni, ba chiar au auzit despre ea și nematematicienii. Pînă și poeții o amintesc ; într-o celebră poezie, Valerii Briusov scrie :

...Dar în fața lui Edip este taina Sfinxului :

Numerele prime tot nu au fost aflate încă...

Să studiem un exemplu care ne va permite să înțelegem punerea problemei. Fie progresia geometrică infinită

$$\div 1, 2, 4, 8, 16, 32, \dots$$

unde fiecare număr este dublul celui precedent. Numărul termenilor este infinit. Cum se dispun aceste numere în raport cu șirul tuturor numerelor naturale? Se vede ușor că, la început, ele „se așază” foarte des: în intervalul de la 1 la 10 sînt patru dintre aceste numere (1, 2, 4, 8). Apoi din ce în ce mai rar. Astfel, în intervalul de la 30 la 40 este numai unul singur (32); în sfîrșit, intervalul de la 1025 pînă la 2025 nu conține nici un număr al șirului nostru. Se arată ușor că, dacă mergem destul de departe în șirul natural, putem găsi un interval oricît de lung, „o insulă”, care să nu conțină nici un termen al progresiei noastre.

Aceasta are o mare asemănare cu proprietățile numerelor prime. Dar există și o diferență esențială. Legea de distribuție a numerelor din șirul 1, 2, 4, 8, 16, ..., în șirul numerelor naturale este foarte simplă. Putem scrie o formulă, cu ajutorul căreia să aflăm numărul termenilor din acest șir, cuprinși între două numere naturale arbitrare. În adevăr, numărul de termeni din șirul nostru care nu depășesc numărul N este egal cu caracteristica logaritmului în baza doi al numărului N , la care se adaugă o unitate (cititorul obișnuit cu logaritmi va efectua singur demonstrația).

Dimpotrivă, legea de distribuție a numerelor din șirul numerelor prime

2, 3, 5, 7, 11, 13, ...

este extrem de complicată: după un șir lung de numere neprime, poate urma un șir bogat în numere prime. De exemplu după intervalul de 11 numere neprime

998, 999, 1000, 1001, 1002, 1003, 1004, 1005, 1006, 1007, 1008, urmează intervalul

1009, 1010, 1011, 1012, 1013, 1014, 1015, 1016, 1017, 1018, 1019,

de asemenea din 11 numere, care conține însă trei numere prime: 1009, 1013 și 1019.

Am văzut că intervalele dintre numerele prime devin din ce în ce mai mari pentru a ajunge, în cele din urmă, oricît de lungi. Dar se întîlnesc iarăși, destul de departe, „aglomerații” neașteptate de numere prime. De exemplu în vecinătatea lui 1000, după un șir de 11 numere neprime, urmează un altul tot de 11 numere, dintre care trei sînt prime. Așadar, la 22 de numere revin trei numere prime, adică peste 13%, ceea ce nu este chiar puțin! Există motive să credem că în șirul numerelor naturale se întîl-

nesc, oricît de departe, perechi de numere prime vecine, despre care am vorbit și în capitolul precedent. De aceea existența unor imense „insule” care nu cuprind numere prime nu ne ajută să ne facem o idee asupra frecvenței lor printre toate numerele naturale. Și totuși...

...Și totuși încă Euler (1707—1783), cel mai de seamă matematician al secolului al XVIII-lea¹⁾, era de părere că numerele prime apar „infinit mai rar decît numerele întregi”. Cum să înțelegem aceste cuvinte ale lui Euler? Iată ce semnificație au. Să considerăm un număr natural N , prim sau neprim. Fie

2, 3, 5, ..., p

toate numerele prime care nu depășesc pe N . (Dacă N este prim, atunci ultimul număr din acest șir va fi $N=p$; în caz contrar p va fi un număr prim mai mic decît N). Să presupunem că obținem în total n numere prime care nu depășesc pe N . De exemplu, considerăm $N=10$; atunci numerele prime mai mici decît 10 vor fi 2, 3, 5, 7, adică în total patru numere; deci $n=4$. Cititorul se va convinge singur că pentru $N=19$, $n=8$; pentru $N=30$, $n=10$ etc.

Numărul n însuși nu ne oferă prea multe informații asupra problemei care ne interesează, însă raportul n/N caracterizează complet desimea sau, exprimat în limbaj științific, „densitatea” numerelor prime printre cele naturale. În tabela următoare sînt date unele valori ale lui N și valorile corespunzătoare pentru n și n/N . În ultima linie se indică raportul n/N în procente:

N	10	100	1 000	100 000	1 000 000	1 000 000 000
n	4	25	168	9 592	78 498	50 847 478
n/N	0,4	0,25	0,168	0,095 92	0,078 498	0,050 847 478
$\frac{n}{N}$, în %	40%	25%	≈ 17%	≈ 9,6%	≈ 8%	≈ 5%

Se observă că „densitatea” numerelor prime în șirul tuturor numerelor naturale devine din ce în ce mai mică, dacă considerăm intervale numerice din ce în ce mai mari.

Cuvintele lui Euler: „numerele prime apar infinit mai rar decît cele întregi”, trebuie înțelese astfel: dacă vom considera un

¹⁾ Euler a trăit și a lucrat peste 30 ani în Rusia, ca membru al Academiei de Științe din Petersburg.

număr N foarte mare de numere naturale consecutive, atunci raportul n/N va fi un număr foarte mic; mai exact, dacă vom alege o valoare foarte mică pentru n/N , de exemplu o milionime, o miliardime etc., vom putea găsi întotdeauna un număr natural mare astfel încât, pentru toate numerele inferioare lui N raportul n/N să fie mai mic decât fracția mică dată.

Euler nu a dat o demonstrație pe deplin riguroasă pentru afirmația sa. Prima demonstrație ireproșabilă a acestei teoreme se datorește matematicianului francez A. M. Legendre, care a publicat-o în 1798.

Așadar, s-a stabilit doar că densitatea numerelor prime descrește indefinit când crește numărul N .

Matematicienii și-au pus următoarea problemă: *să se calculeze n , când N este dat. Cu alte cuvinte, se cere să se găsească o expresie analitică (o formulă) ce dă numărul de numere prime inferioare unui număr natural dat.*

Această problemă nu a putut fi rezolvată nici cu ajutorul aparatului matematic actual. De aceea a fost înlocuită prin alte două probleme: în primul rând, s-a căutat o formulă pentru aflarea lui n dacă N este dat, însă astfel ca eroarea să fie cu atât mai mică cu cât N este mai mare (formula fiind aproximativă); în al doilea rând, s-au căutat legile cărora li se supun abaterile acestei formule, de la legea adevărată a distribuției numerelor prime. Aceste două probleme au o vechime de un secol și jumătate și au preocupat pe cei mai buni matematicieni.

Prima formulă simplă, care exprimă aproximativ numărul de numere prime mai mici decât un număr natural N dat, a fost obținută de Legendre; el a obținut-o „prin încercări”. Această formulă determină destul de bine pe n , pentru orice N mai mare decât 1 000 și mai mic decât 400 000 (în timpul lui Legendre tabelele de numere prime ajungeau numai până la $N=400\,000$; în prezent ciurul lui Eratostene a fost prelungit până la $N=9\,000\,000$).

Iată formula lui Legendre:

$$n = \frac{N}{2,3025 \lg N - 1,08366},$$

unde se ia, bineînțeles, partea întreagă a fracției supraunitare, care se obține pe baza acestei formule. Să considerăm tabela care dă valorile lui n , corespunzătoare diferitelor valori ale lui N , calculate după formula lui Legendre și cele observate direct.

N	10	100	1 000	10 000	100 000
n (după Legendre)	8	28	171	1 230	9 587
n (observat)	4	25	168	1 229	9 592

Începînd cu $N=1\,000$, valorile observate ale lui n și cele calculate sînt foarte apropiate unele de altele, abaterile fiind atît de o parte, cît și de cealaltă: pentru unele valori ale lui N valoarea observată este cu puțin mai mare decât cea calculată, pentru alte valori ea este cu puțin mai mică. Valabilitatea formulei lui Legendre nu a putut fi demonstrată în formă generală nici de el, nici de alți matematicieni.

Pe la jumătatea secolului trecut, interesul pentru problemele teoriei numerelor a crescut considerabil. Un rol important l-au jucat lucrările lui Lejeune-Dirichlet (1805—1859). Dirichlet s-a ocupat mai ales de analiza matematică (capitolele din matematică în care se studiază mărimile cu variație continuă: calculul diferențial, calculul integral etc.). Între altele însă el s-a preocupat și de teoria numerelor. Aplicînd în mod consecvent metodele analizei la teoria numerelor (în această consistă marele său merit), Dirichlet a obținut o seamă de rezultate interesante. Am mai arătat că el a demonstrat valabilitatea mării teoreme a lui Fermat pentru $n=5$ și $n=14$ și că tot el a demonstrat existența unei infinități de numere prime în orice progresie aritmetică în care primul termen și rația sînt prime între ele. Tot el a obținut importante rezultate în teoria ecuațiilor nedeterminate de gradul al doilea. După inițiativa lui Dirichlet¹⁾, matematicienii din diferite țări au început să aplice metodele analitice în studiul numerelor naturale.

Ținînd seama de ciurul lui Eratostene, matematicianul francez Bertrand a emis ipoteza că între orice număr și dublul său există cel puțin un număr prim. (Mai exact, dacă $2x > 7$, atunci între x și $2x-2$ există întotdeauna un număr prim.) Bertrand nu a putut demonstra această propoziție, însă pe baza ei a demonstrat mai multe teoreme importante din aritmetică și din algebră. Ipoteza că între numerele x și $2x$ (pentru $x > 1$) există cel puțin un număr prim a fost denumită de matematicieni „postulatul lui

¹⁾ Dirichlet a fost primul care a aplicat sistematic metodele analizei matematice la studiul numerelor naturale. Anumite rezultate fuseseră obținute pe această cale și înainte, de către Euler și Gauss.

Bertrand¹⁾. „Postulatul” lui Bertrand a putut fi demonstrat de către Cebîșev, în 1852.

P. L. Cebîșev (1821—1894) este considerat pe bună dreptate ca o mîndrie a științei ruse. El a lucrat timp de o jumătate de secol în cele mai variate domenii ale matematicii, obținînd pretutindeni rezultate remarcabile. Însă cel mai important lucru din activitatea sa este faptul că a pus probleme cu totul noi, care au atras repede atenția multor matematicieni și, în primul rînd, atenția elevilor săi. El a creat școala matematică rusă, ai cărei reprezentanți ocupă pînă astăzi un loc conducător în știință.

Cebîșev nu a reușit să găsească o formulă care să dea exact valoarea „densității” n/N pentru un N dat. Am mai spus că și astăzi, la o sută de ani după lucrările lui Cebîșev din domeniul teoriei numerelor, această problemă se consideră irezolubilă (prin mijloacele științei actuale, bineînțeles; este în afară de orice îndoială că știința viitorului va ști s-o rezolve). Însă Cebîșev a demonstrat că, pentru valori foarte mari ale lui N , raportul n/N diferă foarte puțin de mărimea $\frac{0,434\ 29\dots}{\lg N}$, precizia formulei fiind

cu atît mai mare cu cît sînt mai mari valorile considerate ale lui N . Astfel de formule, valabile numai aproximativ, însă care dau o precizie cu atît mai mare cu cît sînt mai mari valorile mărimilor ce intervin în ele, se numesc formule asimptotice. Prin urmare, putem spune că Cebîșev a dat o formulă asimptotică pentru densitatea distribuției numerelor prime. Tot el a obținut o formulă asimptotică pentru calculul numărului n de numere prime care sînt mai mici decît un număr N dat; deoarece în această formulă intervine semnul integrării, nu o vom da aici.

Pe bună dreptate Cebîșev este considerat creatorul legilor asimptotice de distribuție a numerelor prime. El a avut un predecesor care a găsit pe cale pur empirică (prin examinarea minuțioasă a ciurului lui Eratostene) aceleași formule, dar acest predecesor nu a putut să le demonstreze valabilitatea și nu le-a publicat. Este vorba de Gauss.

După descoperirea formulelor asimptotice, s-a pus problema preciziei lor și a legilor care guvernează abaterile valorilor observate ale numărului n , față de cele calculate după aceste formule. De aceste probleme s-au ocupat Cebîșev, Hadamard și Landau, iar în ultimul timp matematicienii englezi Hardy și Littlewood. Problema abaterilor de la formulele lui Cebîșev s-a dovedit a fi extrem de dificilă. Dar și aici s-au obținut unele rezultate.

¹⁾ Cuvîntul latin „postulatum” înseamnă „cerere”. În manualele vechi, enunțul axiomelor începea de obicei cu formularea „vom cere ca...”.

În tabela de mai jos, în prima linie sînt date valorile numerelor naturale, notate cu litera N , în a doua, valorile lui n corespunzătoare, calculate după formula lui Cebîșev și notate cu litera A ; în sfîrșit, în linia a treia sînt date valorile exacte ale lui n .

N	2	5	10	100	1 000	10 000	100 000	1 000 000	10 000 000	100 000 000
A	1	4	6	29	178	1 246	9 630	78 623	664 918	5 762 209
n	1	3	4	25	168	1 229	9 592	78 498	664 579	5 761 455

Se observă că diferența dintre A și n crește odată cu creșterea lui N , însă raportul dintre această diferență și N scade repede. De exemplu pentru $N=1\,000$, avem

$$A-n=178-168=10$$

(10 reprezintă 1/10% din 1 000), iar pentru $N=1\,000\,000$

$$A-n=78\,628-78\,498=130$$

(mai mare decît pentru $N=1\,000$). Însă, în raport cu milionul de numere considerate, 130 reprezintă doar 0,013%, adică aproximativ de opt ori mai puțin decît în cazul $N=1\,000$. Prin urmare, acest raport caracterizează calitatea unei relații aproximative. Se vede că pentru formula lui Cebîșev acest raport este mic; prin urmare, formula este bună: cu cît sînt mai mari numerele considerate, cu atît formula dă rezultate mai bune (lege asimptotică).

Pe de altă parte, observăm că A este totdeauna mai mare decît n , ceea ce este valabil nu numai pentru numerele cuprinse în tabela noastră, ci și pentru orice N căruia îi corespunde un A și un n . Era firesc să se creadă că formula lui Cebîșev dă întotdeauna un rezultat întrucîtva „mărit”. Pînă în 1914 s-au făcut numeroase încercări de a demonstra această afirmație, adică de a demonstra că $A \geq n$ pentru N arbitrar. Însă, în 1914, Littlewood a arătat că există numere (valori ale lui N), pentru care n trebuie în mod necesar să fie mai mare decît A ; pentru valori și mai mari ale lui N vom întîlni atît valori ale lui N pentru care $A > n$, cît și valori pentru care $n > A$. Cu alte cuvinte, abaterile de la formula lui Cebîșev vor fi nu numai infime, ci vor avea totodată și un caracter complet întîmplător, oscilînd în jurul valorilor reale.

Care este cel mai mic număr natural pentru care formula lui Cebîșev dă un rezultat mai mic decît cel real? Matematicianul Hardy, colaborator al lui Littlewood, a arătat că acest număr este enorm de mare; el a putut să precizeze că este mai mic decît 10^{700} . Se părea că va fi imposibil să ne apropiem de acest număr. Abia recent, în 1933, matematicianul englez Skews a reușit să demonstreze că (dacă se face anumite ipoteze suplimentare) se poate evalua numărul pentru care formula lui Cebîșev dă primul număr din șirul numerelor naturale mai mic decît cel real. Acest număr este aproximativ egal cu $10^{10^{10^{34}}}$.

Numărul lui Skews este considerabil mai mare decît toate numerele gigante menționate pînă acum și poate fi considerat, în acest sens, drept un „număr record”. Numărul 99^9 , despre care a fost vorba în primul capitol, și chiar numărul imens $10^8 \cdot 10^{16}$ din „Psammit”, sînt foarte foarte mici în comparație cu gigantul lui Skews.



CAPITOLUL XIII

PROBLEMA LUI GOLDBACH



În capitolul precedent am analizat problema distribuției numerelor prime printre toate numerele naturale. Am constatat că numerele prime apar relativ des la începutul șirului numerelor naturale și devin apoi din ce în ce mai rare, adică intervalele dintre ele se măresc. În aceste intervale există numere care sînt suma a două numere prime. Iată de exemplu numerele pînă la zece: 1 (nu intră în considerație); 2 (prim); 3 (prim); 4 ($2+2$, suma a două numere prime); 5 (prim); 6 ($3+3$, suma a două numere prime); 7 (prim); 8 ($3+5$, suma a două numere prime); 9 ($2+7$, suma a două numere prime); 10 ($3+7$, suma a două numere prime). Prin urmare, toate numerele pînă la 10 sînt sau prime sau sumă a două numere prime. Însă 27, de exemplu, nu mai poate fi reprezentat sub forma unei sume de două numere prime, ci ca o sumă a trei numere prime: $27=3+11+13$. Pentru ce număr natural nu vor mai fi suficiente trei numere prime? Care este numărul minim format din cel puțin patru, cinci etc. numere prime?

Astfel de probleme pot fi extinse. Matematicienii se interesează de multă vreme de felul în care se poate scrie un număr ca sumă a mai multor pătrate. Dacă acest lucru este posibil, atunci în cîte moduri se realizează descompunerea respectivă? Aceleași probleme se pot pune și la descompunerea unui număr într-o sumă de cuburi etc. Apare astfel un domeniu special al teoriei numerelor, în care locul divizorilor și al factorilor este luat de termeni și sume. Acest domeniu se numește teoria aditivă a numerelor, denumire care vine de la cuvîntul

latinesc „additio“ (adunare). În ceea ce privește partea din teoria numerelor care se ocupă cu factori și divizori (teoria divizibilității etc.), ea se numește teoria multiplicativă a numerelor (de la cuvântul latinesc „multiplicatio“ care înseamnă înmulțire).

Să revenim la problema reprezentării oricărui număr sub forma unei sume de mai multe numere prime. Ea a preocupat acum mai bine de 200 de ani pe Chr. Goldbach, membru al Academiei de Științe din Petersburg. Goldbach a considerat foarte multe numere, încercând să le descompună într-o sumă de numere prime și a ajuns la convingerea că trei termeni sînt totdeauna suficienți. Deoarece nu a putut să demonstreze această propoziție, el i-a scris prietenului său Euler, cu care era în corespondență de aproape 15 ani și care se afla atunci în culmea gloriei. Într-o scrisoare din 7 iunie 1742, Goldbach îi comunica lui Euler că îndrăznește să enunțe următoarea ipoteză: „orice număr mai mare decît cinci este suma a trei numere prime“. Euler i-a răspuns că el consideră perfect adevărată teorema care spune că: orice număr par este suma a două numere prime. De aici, ca o consecință simplă, se obține afirmația lui Goldbach (cititorul va răspunde de ce). De altfel nici Euler nu a dat o demonstrație.

Așadar, s-a pus următoarea problemă (numită problema lui Goldbach): să se demonstreze sau să se infirme propoziția „*orice număr mai mare decît unitatea este suma a cel mult trei numere prime*“. Nici contemporanii lui Goldbach și Euler, nici chiar matematicienii din secolul trecut, nu au putut să rezolve problema. G. Cantor, unul dintre cei mai originali matematicieni ai secolului trecut, a avut răbdarea să încerce toate numerele pare de la 2 pînă la 1000, iar Aubry de la 1000 pînă la 2000; ei s-au convins că între aceste limite orice număr par este suma a două numere prime. În 1911, E. Melet a arătat că majoritatea covârșitoare a numerelor pare cuprinse între 4 și 9000 000 sînt sume a cîte două numere prime; numărul excepțiilor nu poate fi mai mare de patrusprezece (deci, pentru 4499 986 de numere pare, afirmația lui Goldbach este cu siguranță adevărată). În sfîrșit, la începutul secolului al XX-lea au apărut mai multe lucrări care încercau să traseze căile pentru rezolvarea acestei probleme sau să o lege de alte probleme ale matematicii. Însă demonstrarea ei riguroasă a rămas tot în sus-

pensie. În 1912 E. Landau a emis ipoteza că această problemă nu se poate rezolva cu mijloacele „actuale“ ale matematicii!...

În 1923 matematicienii englezi Hardy și Littlewood au realizat un oarecare progres în încercările de a găsi o soluție problemei lui Goldbach. Ei au reușit să lege problema lui Goldbach de una dintre cele mai dificile și mai interesante probleme ale teoriei funcțiilor analitice (un capitol special din matematica superioară). Nici această problemă nu este rezolvată, nu este dusă pînă la capăt, însă legătura descoperită între aceste două ramuri ale științei, în aparență de naturi diferite, s-a dovedit fecundă și a dus la o serie de descoperiri.

O cotitură hotărîtoare s-a produs în 1930. Marele matematician sovietic L. G. Șnirelman (1905—1938) a reușit să modifice astfel problema, încît a rezolvat-o prin mijloace inventate tot de el. Anume, constatînd că încercările anterioare de a demonstra sub forma inițială nu au dat rezultate, Șnirelman „a slăbit“, cum spun matematicienii, condițiile problemei lui Goldbach, ceea ce a dus la o problemă înrudită, considerabil mai simplă. Goldbach cerea să se demonstreze că orice număr natural este suma a cel mult trei numere prime. Se poate cere ca orice număr natural să fie suma a cel mult patru, cinci, ..., o sută de numere prime. Evident, aceste condiții sînt mai slabe decît cele ale lui Goldbach; în adevăr, un număr care se descompune într-o sută de numere prime ar putea să nu se descompună într-o sumă de trei.

În sfîrșit, se poate pune problema cum a procedat Șnirelman: *există oare un număr întreg pe deplin determinat, însă necunoscut (il vom nota cu litera C), astfel încît orice număr natural să poată fi reprezentat sub forma a cel mult C termeni primi?*

Cu alte cuvinte, oricare ar fi numărul natural N , se poate scrie totdeauna

$$N = p_1 + p_2 + p_3 + \dots + p_n,$$

unde $p_1, p_2, \dots, p_n$ sînt numere prime, iar n este cu siguranță mai mic decît C (cel mult egal cu el). Dacă se va putea demonstra că $C=3$, afirmația lui Goldbach va fi demonstrată. Șnirelman a reușit să demonstreze complet această teoremă „atenuată“. Numărul C , deocamdată necunoscut, se numește, de atunci, „numărul lui Șnirelman“ sau „constantă lui Șnirelman“. Așadar, afirmația lui Goldbach poate fi enunțată și astfel: „constantă lui Șnirelman este egală cu trei“. Însă aceasta este prea puțin.

Analiza cea mai exactă a metodei lui Șnirelman, efectuată de alți matematicieni (Romanov, Landau, Heilborn, Ricii), a permis să se obțină o evaluare a constantei lui Șnirelman; foarte mare la început, ea a fost redusă treptat pînă la 67.

Desigur de aici mai este foarte mult pînă la numărul 3 al lui Goldbach. Important este însă că aceasta s-a demonstrat pentru numere arbitrare, oricît ar fi de mari. Despre un număr oarecare, cum ar fi de exemplu

835 042 000 000 000 000 000 000 000,

sau vechea noastră cunoștință 99^9 , pentru a cărei scriere sînt necesare 30 de volume, putem afirma în egală măsură că 67 de termeni primi sînt suficienți pentru a-l reprezenta. Chiar gigantul $10^{10^{34}}$ al lui Skews poate fi reprezentat, pe baza demonstrației lui Șnirelman, sub forma unei sume de cel mult 67 numere prime (unii dintre acești termeni vor fi și ei imens de mari, mult mai mari decît 99^9). Prin urmare, rezultatul lui Șnirelman este o realizare uriașă. Principalul este că s-au deschis căi noi, s-au descoperit noi posibilități pentru a aborda rezolvarea unei vechi probleme. Așadar, se puteau aștepta și rezultate noi. Așa s-a întîmplat în realitate.

În 1937, academicianul I. M. Vinogradov, Erou al Muncii Socialiste și Laureat al Premiului Stalin, încă pe atunci celebru în lumea întreagă prin lucrările sale din domeniul teoriei aditive a numerelor, a rezolvat aproape complet problema lui Goldbach, care fusese considerată cu puțin înainte ca inaccesibilă.

Rezultatul obținut de I. M. Vinogradov poate fi enunțat astfel: pentru toate numerele impare, destul de mari, problema lui Goldbach este complet rezolvată. Sau altă formulare: constanta lui Șnirelman pentru numere impare destul de mari nu este mai mare decît 3.

De ce nu poate fi considerată soluția lui I. M. Vinogradov ca soluție completă, definitivă, a problemei lui Goldbach? De ce am afirmat că el a rezolvat „aproape” complet această problemă? Am văzut că Euler și Goldbach au afirmat că orice număr par este suma a două numere prime (aceasta s-a confirmat experimental pentru numere relativ mici). De aici rezultase, ca o consecință, că orice număr impar este suma a cel mult trei numere prime. Vinogradov a demonstrat ultima afirmație despre numerele impare; de aici urmează imediat că pentru orice număr par sînt suficienți patru termeni primi (numere prime). Rămîne însă deschisă problema dacă sînt suficienți doi termeni. În afară de

aceasta, după Vinogradov, afirmația lui Goldbach este valabilă pentru toate numerele impare destul de mari, adică începînd cu un număr mare rămas cîtva timp necunoscut.

În 1939 acest număr a fost calculat de către tînărul matematician sovietic K. G. Borozdkin:

$e^{e^{41,96}}$,

unde numărul e este baza logaritmilor naturali ($e=2,7182\dots$). Trebuia să se micșoreze considerabil numărul găsit de K. G. Borozdkin, după care să se verifice direct toate numerele mai mici. Această lucrare a fost efectuată de Cantor și de Aubry, însă numai pentru numerele pînă la 2000.

Am insistat asupra problemei lui Goldbach pentru că este foarte interesantă din diferite puncte de vedere și pentru că știința rusă are dreptul să se mîndrească cu ea. Această problemă îi aparține matematicianului Goldbach; primul progres în rezolvarea ei se datorește lui L. G. Șnirelman, iar soluția ei a fost obținută de academicianul I. M. Vinogradov.



Tabela numerelor prime mai mici decit 6 000

2	331	751	1 217	1 697	2 221	2 719	3 299	3 803	4 357	4 943	5 503
3	337	757	1 223	1 699	2 237	2 729	3 301	3 821	4 363	4 951	5 507
5	347	761	1 229	1 709	2 239	2 731	3 307	3 823	4 373	4 957	5 519
7	349	769	1 231	1 721	2 243	2 741	3 313	3 833	4 391	4 967	5 521
11	353	773	1 237	1 723	2 251	2 749	3 319	3 847	4 397	4 969	5 527
13	359	787	1 249	1 733	2 267	2 753	3 323	3 851	4 409	4 973	5 531
17	367	797	1 259	1 741	2 269	2 767	3 329	3 853	4 421	4 987	5 557
19	373	809	1 277	1 747	2 273	2 777	3 331	3 863	4 423	4 993	5 563
23	379	811	1 279	1 753	2 281	2 789	3 343	3 877	4 441	4 999	5 569
29	383	821	1 283	1 759	2 287	2 791	3 347	3 881	4 447	5 003	5 573
31	389	823	1 289	1 777	2 293	2 797	3 359	3 889	4 451	5 009	5 581
37	397	827	1 291	1 783	2 297	2 801	3 361	3 907	4 457	5 011	5 591
41	401	829	1 297	1 787	2 309	2 803	3 371	3 911	4 463	5 021	5 623
43	409	839	1 301	1 789	2 311	2 819	3 373	3 917	4 481	5 023	5 639
47	419	853	1 303	1 801	2 333	2 833	3 389	3 919	4 483	5 039	5 641
53	421	857	1 307	1 811	2 339	2 837	3 391	3 923	4 493	5 051	5 647
59	431	859	1 319	1 823	2 341	2 843	3 407	3 929	4 507	5 059	5 651
61	433	863	1 321	1 831	2 347	2 851	3 413	3 931	4 513	5 077	5 653
67	439	877	1 327	1 847	2 351	2 857	3 433	3 943	4 517	5 081	5 657
71	443	881	1 361	1 861	2 357	2 861	3 449	3 947	4 519	5 087	5 659
73	449	883	1 367	1 867	2 371	2 879	3 457	3 967	4 523	5 099	5 669
79	457	887	1 373	1 871	2 377	2 887	3 461	3 989	4 547	5 101	5 683
83	461	907	1 381	1 873	2 381	2 897	3 463	4 001	4 549	5 107	5 689
89	463	911	1 399	1 877	2 383	2 903	3 467	4 003	4 561	5 113	5 693
97	467	913	1 409	1 879	2 389	2 909	3 469	4 007	4 567	5 119	5 701
101	479	929	1 423	1 889	2 393	2 917	3 491	4 013	4 583	5 147	5 711
103	487	937	1 427	1 901	2 399	2 927	3 499	4 019	4 591	5 153	5 717
107	491	941	1 429	1 907	2 411	2 939	3 511	4 021	4 597	5 167	5 737
109	499	947	1 433	1 913	2 417	2 953	3 517	4 027	4 603	5 171	5 741
113	503	953	1 439	1 931	2 423	2 957	3 527	4 049	4 621	5 179	5 743
127	509	967	1 447	1 933	2 437	2 963	3 529	4 051	4 637	5 189	5 749
131	521	971	1 451	1 949	2 441	2 969	3 533	4 057	4 639	5 197	5 779
137	523	977	1 453	1 951	2 447	2 971	3 539	4 073	4 643	5 209	5 783
139	541	983	1 459	1 973	2 459	2 999	3 541	4 079	4 649	5 227	5 791
149	547	991	1 471	1 979	2 467	3 001	3 547	4 091	4 651	5 231	5 801
151	557	997	1 481	1 987	2 473	3 011	3 557	4 093	4 657	5 233	5 807
157	563	1 009	1 483	1 993	2 477	3 019	3 559	4 099	4 663	5 237	5 813
163	569	1 013	1 487	1 997	2 503	3 023	3 571	4 111	4 673	5 261	5 821
167	571	1 019	1 489	1 999	2 521	3 037	3 581	4 127	4 679	5 273	5 827
173	577	1 021	1 493	2 003	2 531	3 041	3 583	4 129	4 691	5 279	5 839
179	587	1 031	1 499	2 011	2 539	3 049	3 593	4 133	4 703	5 281	5 843
181	593	1 033	1 511	2 017	2 543	3 061	3 607	4 139	4 721	5 297	5 849
191	599	1 039	1 523	2 027	2 549	3 067	3 613	4 153	4 723	5 303	5 851
193	601	1 049	1 531	2 029	2 551	3 079	3 617	4 157	4 729	5 309	5 857
197	607	1 051	1 543	2 039	2 557	3 083	3 623	4 159	4 733	5 323	5 861
199	613	1 061	1 549	2 053	2 579	3 089	3 631	4 177	4 751	5 333	5 867
211	617	1 063	1 553	2 063	2 591	3 109	3 637	4 201	4 759	5 347	5 869
223	619	1 069	1 559	2 069	2 593	3 119	3 643	4 211	4 783	5 351	5 879
227	631	1 087	1 567	2 081	2 609	3 121	3 659	4 217	4 787	5 381	5 881
229	641	1 091	1 571	2 083	2 617	3 137	3 671	4 219	4 789	5 387	5 897
233	643	1 093	1 579	2 087	2 621	3 163	3 673	4 229	4 793	5 393	5 903
239	647	1 097	1 583	2 089	2 633	3 167	3 677	4 231	4 799	5 399	5 923
241	653	1 103	1 597	2 099	2 647	3 169	3 691	4 241	4 801	5 407	5 927
251	659	1 109	1 601	2 111	2 657	3 181	3 697	4 243	4 813	5 413	5 939
257	661	1 117	1 607	2 113	2 659	3 187	3 701	4 253	4 817	5 417	5 953
263	673	1 123	1 609	2 129	2 663	3 191	3 709	4 259	4 831	5 419	5 981
269	677	1 129	1 613	2 131	2 671	3 203	3 719	4 261	4 861	5 431	5 987
271	683	1 151	1 619	2 137	2 677	3 209	3 727	4 271	4 871	5 437	
277	691	1 153	1 621	2 141	2 683	3 217	3 733	4 273	4 877	5 441	
281	701	1 163	1 627	2 143	2 687	3 221	3 739	4 283	4 889	5 443	
283	709	1 171	1 637	2 153	2 689	3 229	3 761	4 289	4 903	5 449	
293	719	1 181	1 657	2 161	2 693	3 251	3 767	4 297	4 909	5 471	
307	727	1 187	1 663	2 179	2 699	3 253	3 769	4 327	4 919	5 477	
311	733	1 193	1 667	2 203	2 707	3 257	3 779	4 337	4 931	5 479	
313	739	1 201	1 669	2 207	2 711	3 259	3 793	4 339	4 933	5 483	
317	743	1 213	1 693	2 213	2 713	3 271	3 797	4 349	4 937	5 501	

TABLA DE MATERII

Din prefața autorului la prima ediție	3
Introducere	5
Capitolul I: Sistemul nostru de numerație	7
Capitolul II: Cum numărau strămoșii noștri?	16
Capitolul III: De ce a numărat Arhimede firele de nisip și cum le-a numărat?	26
Capitolul IV: Nu cite zece, ci cite cinci sau cite douăsprezece	31
Capitolul V: O aritmetică în care nu trebuie să socotim	39
Capitolul VI: Măsura comună	48
Capitolul VII: Ecuatiile pe care le studiază aritmetica	61
Capitolul VIII: O aritmetică în care „trei ori trei fac patru”	82
Capitolul IX: Divizibil sau nu?	97
Capitolul X: Iarăși despre divizibilitate, o teoremă „mare”, cunoscută sub numele de „mica teoremă”	106
Capitolul XI: Ciurul lui Eratostene	116
Capitolul XII: Des ori rar?	129
Capitolul XIII: Problema lui Goldbach	137
Anexă: Tabela numerelor prime mai mici decit 6 000	142